Low-Coherence Frames from Group Fourier Matrices

Matthew Thill   Babak Hassibi

Department of Electrical Engineering, Caltech, Pasadena, CA

Abstract

Many problems in areas such as compressive sensing and coding theory seek to design a set of equal-norm vectors with large angular separation. This idea is essentially equivalent to constructing a frame with low coherence. The elements of such frames can in turn be used to build high-performance spherical codes, quantum measurement operators, and compressive sensing measurement matrices, to name a few applications.

In this work, we allude to the group-frame construction first described by Slepian and further explored in the works of Vale and Waldron. We present a method for selecting representations of a finite group to construct a group frame that achieves low coherence. Our technique produces a tight frame with a small number of distinct inner product values between the frame elements, in a sense approximating a Grassmanian frame. We identify special cases in which our construction yields some previously-known frames with optimal coherence meeting the Welch lower bound, and other cases in which the entries of our frame vectors come from small alphabets. In particular, we apply our technique to the problem choosing a subset of rows of a Hadamard matrix so that the resulting columns form a low-coherence frame. Finally, we give an explicit calculation of the average coherence of our frames, and find regimes in which they satisfy the Strong Coherence Property described by Mixon, Bajwa, and Calderbank.

Index Terms

Frame, coherence, unit norm tight frame, group representation, group frame, Fourier transform over groups, Welch bound, spherical codes, compressive sensing.

I. Introduction:

Matrix Coherence and Frames

Recall that a set of vectors $\{f_i\}_{i=1}^n$ in $\mathbb{C}^m$ (respectively $\mathbb{R}^m$) forms a *frame* if there are two positive constants A and B such that for any $f \in \mathbb{C}^m$ (respectively $\mathbb{R}^m$), we have

$$A||f||^2 \leq \sum_{i=1}^{n} |\langle f, f_i \rangle|^2 \leq B||f||^2. \tag{1}$$

If we arrange our frame elements to be the columns of a matrix $\mathbf{M} = [f_1, ..., f_n]$, the frame is said to be *tight* if $\mathbf{M}\mathbf{M}^* = \lambda \mathbf{I}$, where λ is a real scalar and $\mathbf{I}$ is the $m \times m$ identity matrix. This is equivalent to having $A = B$ in (1), and we can see that in this case we necessarily have $A = B = \lambda$. The frame is called *unit norm* if $||f_i|| = 1$, $\forall i$, and a tight unit-norm frame satisfies $\mathbf{M}\mathbf{M}^* = \frac{n}{m}\mathbf{I} \in \mathbb{C}^{m \times m}$. We will typically restrict our attention to unit-norm frames.

Of particular interest in frame design are the magnitudes of the inner products between distinct frame elements, $|\langle f_i, f_j \rangle|$, $i \neq j$. A unit-norm frame is called *equiangular* if all of these magnitudes are equal: $|\langle f_i, f_j \rangle| = \alpha$, $\forall i \neq j$, for some constant α. In general, we would like all of the inner product magnitudes to be as small as possible so that the frame vectors are well-spaced about the m-dimensional unit sphere. Such frames popularly have applications to coding theory (for instance, spherical codes [14], [32] and LDPC codes [20]) and compressive sensing [4]–[6], [17], [18], [40]. They also arise in areas such as quantum measurements [19], [28], [29] and MIMO communications [23], [24]. Recently, frame theory itself has proven to be an exciting field, and has been notably studied by Casazza, Kutyniok, Fickus, Dixon, and others [7]–[9], [11], [12], [21].

On this note, let us formalize our particular problem: We would like to minimize the *coherence* μ of a unit-norm frame defined as the largest inner product magnitude between two distinct frame elements:

$$\mu := \max_{i \neq j} |\langle f_i, f_j \rangle|. \tag{2}$$

The following is a classical lower bound on the coherence due to Welch [46]:

Theorem 1: Let $\{f_i\}_{i=1}^n$ be a unit-norm frame in $\mathbb{C}^m$ or $\mathbb{R}^m$. The coherence $\mu := \max_{i \neq j} |\langle f_i, f_j \rangle|$ satisfies

$$\mu \geq \sqrt{\frac{n-m}{m(n-1)}}, \tag{3}$$

with equality if and only $\{f_i\}$ is both tight and equiangular. In this case, the frame is called *Grassmanian.*

Proof: The bound in (3) is one of a more general set of bounds originally derived by Welch in [46]. This version of the theorem is typically proven (e.g. in [32]) by considering the eigenvalues of the Gram matrix $\mathbf{G} := [\langle f_i, f_j\rangle]$. ■

It should be emphasized that the Welch bound is often quite difficult to achieve with equality, and in fact for certain values of n and m it is impossible to achieve it. So in general, we would like to construct frames which have coherence close to the Welch bound.

If we omit the requirement that our frame be equiangular, we obtain the following relaxation of the Welch bound:

Lemma 1: Let $\{f_i\}_{i=1}^n$ be a unit-norm frame in $\mathbb{C}^m$ or $\mathbb{R}^m$. Then the mean value of the $n(n-1)$ squared inner product norms $\{|\langle f_i, f_j\rangle|^2\}_{i\neq j}$ satisfies

$$\frac{1}{n(n-1)}\sum_{i\neq j}|\langle f_i, f_j\rangle|^2 \geq \frac{n-m}{m(n-1)}, \tag{4}$$

with equality if and only if $\{f_i\}$ is a tight frame.

Proof: The quantity $\frac{1}{n(n-1)}\sum_{i\neq j}|\langle f_i, f_j\rangle|^2$ is very closely related to the *frame potential* defined in [2], and (4) follows from Theorem 6.2 in that work. ■

Lemma 1 allows us to obtain upper bounds on the coherence of tight frames, which become particularly effective when there are few distinct inner product values $\{|\langle f_i, f_j\rangle|\}_{i\neq j}$, with each value arising the same number of times in this set.

Lemma 2: Let $\{f_i\}_{i=1}^n$ be a unit-norm tight frame in $\mathbb{C}^m$ or $\mathbb{R}^m$, such that the inner product norms $\{|\langle f_i, f_j\rangle|\}_{i\neq j}$ take on κ distinct values, with each value arising the same number of times as such an inner product norm. Then the coherence μ of the frame is at most a factor of $\sqrt{\kappa}$ greater than the Welch bound:

$$\mu \leq \sqrt{\kappa}\sqrt{\frac{n-m}{m(n-1)}}. \tag{5}$$

Proof: Consider the squares of the κ distinct inner product values. Since each of these squares arises the same number of times as a squared norm $|\langle f_i, f_j\rangle|^2$, we have that the average $\frac{1}{n(n-1)}\sum_{i\neq j}|\langle f_i, f_j\rangle|^2$ is equal to the mean of the κ squares. By Lemma 1, this mean is equal to $\frac{n-m}{m(n-1)}$. This means that none of the squares can be larger than $\kappa\frac{n-m}{m(n-1)}$, so the coherence is bounded by $\sqrt{\kappa}\sqrt{\frac{n-m}{m(n-1)}}$. ■

When $\kappa = 1$ in Lemma 2, the frame becomes both tight and equiangular, and fittingly the coherence in (5) achieves the Welch bound. In some of our previous work [35], we provided constructions of unit-norm tight frames in which we could control the number of distinct inner product values and ensure that each would arise with the same multiplicity.

In what follows, we will generalize our original construction using a framework which also encompasses some of our subsequent results on frames arising from representations of various groups [36], [38], [39]. Frames constructed in this fashion are called "group frames," and will be reviewed in Section II. In Section III, we will discuss the connection between tight group frames and generalized group Fourier matrices. The problem of designing tight group frames with low coherence is essentially that of choosing a subset of rows of one of these matrices to form a matrix with low coherence. Viewing the problem in this manner allows us to use character theory to design our frames, and leads us to a frame construction that we present in Section V along with bounds on the resulting frame coherence. We explore how this construction performs when using representations of several different types of groups, including general linear groups, vector spaces over finite fields, and special linear groups. We will present methods to maintain low alphabet sizes in our frame entries, sometimes producing frames which can be realized as a subset of rows of a Hadamard matrix (see Section VI-B). In certain cases, we end up with frames arising from difference sets over finite fields, so in some sense we give insight into the frames described in [47] and [15]. Finally, in Section VIII we examine when these frames satisfy the Coherence Property and the Strong Coherence Property described by [1] and [25]. In particular, we utilize the group structure of our frames to calculate their *average coherence* explicitly.

II. Group Frames

One technique first used by Slepian [31] in constructing his "group codes" to reduce the number of inner product values between vectors involves taking the images of a unit-norm vector $\mathbf{v} \in \mathbb{C}^{m\times 1}$ under a finite multiplicative group of unitary matrices $\mathcal{U} = \{\mathbf{U}_1, ..., \mathbf{U}_n\} \subset \mathbb{C}^{m\times m}$. The resulting set of vectors $\{\mathbf{U}_1\mathbf{v}, ..., \mathbf{U}_n\mathbf{v}\}$ has mutual inner products in the form

$$\mathbf{v}^*\mathbf{U}_i^*\mathbf{U}_j\mathbf{v} = \mathbf{v}^*\mathbf{U}_i^{-1}\mathbf{U}_j\mathbf{v} = \mathbf{v}\mathbf{U}_k\mathbf{v}, \tag{6}$$

where we have exploited the fact that $\mathbf{U}_i^{-1}\mathbf{U}_j$ is some other element $\mathbf{U}_k$ of $\mathcal{U}$. This immediately reduces the number of inner product values that can arise from a possible $\binom{n}{2}$ to only at most $n-1$, corresponding to each of the nonidentity group elements of $\mathcal{U}$. (The identity element $\mathbf{U}_1$ is simply the identity matrix $\mathbf{I} \in \mathbb{C}^{m\times m}$. The corresponding inner product $\mathbf{v}^*\mathbf{v} = 1$ arises only when taking the inner product of a vector $\mathbf{U}_i\mathbf{v}$ with itself, and is thus not considered in calculating the coherence of the frame.)

One can quickly verify that each of the values $\mathbf{v}^*\mathbf{U}_k\mathbf{v}$ arises the same number of times as the inner product between two vectors $\mathbf{U}_i\mathbf{v}$ and $\mathbf{U}_j\mathbf{v}$ (since for each $\mathbf{U}_i$ there is exactly one element $\mathbf{U}_j$ that satisfies $\mathbf{U}_i^*\mathbf{U}_j = \mathbf{U}_k$, and it is given by $\mathbf{U}_j := \mathbf{U}_i\mathbf{U}_k$). As a result, the group codes naturally lend themselves to analysis using Lemmas 1 and 2.

Frames arising in this form are called "group frames," and are well-studied in the works of Vale, Waldron, and others [13], [22], [41]–[44]. A great review of group frames is provided in [10].

When $\mathcal{U}$ is chosen to be abelian, so that all the $\mathbf{U}_i$ commute with each other, then the matrices can be simultaneously diagonalized by a unitary change of basis matrix $\mathbf{B}$ so that we may write $\mathbf{B}^*\mathbf{U}_i\mathbf{B} = \mathbf{D}_i$, where $\mathbf{D}_i$ is diagonal. In this case the inner product corresponding to $\mathbf{U}_i$ will take the form

$$\mathbf{v}^*\mathbf{U}_i\mathbf{v} = \mathbf{v}^*\mathbf{B}^*\mathbf{D}_i\mathbf{B}\mathbf{v},$$

so by replacing $\mathbf{v}$ with $\mathbf{B}^*\mathbf{v}$ without loss of generality, we may assume that the $\mathbf{U}_i$ are already diagonal. Furthermore, since each $\mathbf{U}_i$ must have a multiplicative order dividing the size of $\mathcal{U}$, we may take the diagonal entries of $\mathbf{U}_i$ to be powers of the n^{th}-root of unity $\omega := e^{\frac{2\pi i}{n}}$. The matrices will then take the form

$$\mathbf{U}_j = \mathrm{diag}(\omega^{a_{1,j}}, ..., \omega^{a_{m,j}}) \in \mathbb{C}^{m\times m},$$

where the $a_{i,j}$ are integers between 0 and $n-1$. In the language of representation theory, we have decomposed $\mathcal{U}$ into its degree-1 irreducible representations.

If we write the coordinates of our rotated vector as $\mathbf{v} = (v_1, ..., v_m)^T \in \mathbb{C}^{m\times 1}$, then our inner products will now take the form

$$\mathbf{v}^*\mathbf{U}_j\mathbf{v} = \sum_{i=1}^{m} \omega^{a_{i,j}} |v_i|^2, \tag{7}$$

so we see that the inner products depend only on the magnitudes of the v_i, which weight the diagonal entries of the $\mathbf{U}_j$. A natural choice is therefore to choose all the v_i to be real and of equal magnitude (i.e., take $\mathbf{v} := \frac{1}{\sqrt{m}}[1, ..., 1]^T \in \mathbb{C}^{m\times 1}$). When we do this, and in addition require the sets of diagonal components $\{\omega^{a_{i,j}}\}_{i=1}^{m}$ to form distinct representations of $\mathcal{U}$, we obtain what is called a *harmonic frame*, which we will define concretely as follows:

Definition 1: Let m and n be integers, $\omega = e^{\frac{2\pi i}{n}}$, and $\mathbf{U}_j = \text{diag}(\omega^{a_{1,j}}, ..., \omega^{a_{m,j}}) \in \mathbb{C}^{m\times m}$ for $j = 1, ..., n$, where the $a_{i,j}$ are integers between 0 and $n-1$. If we set $\mathbf{v} = \frac{1}{\sqrt{m}}[1, ..., 1]^T \in \mathbb{C}^{m\times 1}$, and $\mathbf{M} = [\mathbf{U}_1\mathbf{v}, ..., \mathbf{U}_n\mathbf{v}]$, then if the rows of $\mathbf{M}$ are distinct, we call the set of columns $\{\mathbf{U}_j\mathbf{v}\}_{j=1}^{n}$ a *harmonic frame*.

Harmonic frames are one of the most thoroughly-studied types of structured frames [13], [22]. As a preliminary result, we have the following:

Lemma 3: A harmonic frame is a tight, unit-norm frame.

Proof: The fact that harmonic frames are unit-norm follows straight from the definition. The rest of this lemma is proven in [10], and we will also explain the tightness of harmonic frames in Section III. ■

An important example of a harmonic frame arises when we choose the group $\mathcal{U}$ to be cyclic, meaning that each $\mathbf{U}_j$ is a power of a single matrix $\mathbf{U} = \text{diag}(\omega^{a_1}, ..., \omega^{a_m})$, so we may write $\mathbf{U}_j := \mathbf{U}^j$. In this case, if we again take $\mathbf{v}$ to be the normalized vector of all 1s, our frame matrix takes the form

$$\mathbf{M} = \begin{bmatrix}\mathbf{v} & \mathbf{U}\mathbf{v} & \dots & \mathbf{U}^{n-1}\mathbf{v}\end{bmatrix} \tag{8}$$

$$= \frac{1}{\sqrt{m}}\begin{bmatrix}1 & \omega^{a_1} & \omega^{a_1\cdot 2} & \dots & \omega^{a_1\cdot(n-1)} \\ 1 & \omega^{a_2} & \omega^{a_2\cdot 2} & \dots & \omega^{a_2\cdot(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{a_m} & \omega^{a_m\cdot 2} & \dots & \omega^{a_m\cdot(n-1)}\end{bmatrix}, \tag{9}$$

where the columns form a harmonic frame precisely when the a_i are distinct. In this form, we see that $\mathbf{M}$ is a subset of rows of the $n\times n$ discrete Fourier matrix, so it becomes clear that the frame is tight since $\mathbf{M}\mathbf{M}^* = \frac{n}{m}\mathbf{I} \in \mathbb{C}^{m\times m}$. The question now becomes how to choose the frequencies a_i to produce frames with low coherence?

In our previous work [35], [36], we developed a method to obtain a range of frames with few distinct inner product values when $\mathcal{U}$ is a cyclic group and $\mathbf{v}$ is the normalized vector of all 1s. We presented resulting upper bounds on the coherence of our frames which came reasonably close to the Welch bound. Our method was simple: choose n to be a prime so that the set of integers $\{1, 2, ..., n-1\}$ forms a cyclic group under multiplication modulo n, denoted $(\mathbb{Z}/n\mathbb{Z})^{\times}$. Then choose m to be a divisor of $n-1$. Since $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is cyclic, it has a unique cyclic subgroup a of size m. We choose the a_i to be the integer elements of this subgroup.

Theorem 2: Let n be a prime, m a divisor of $n-1$, and $A = \{a_i\}_{i=1}^m$ the unique subgroup of $(\mathbb{Z}/n\mathbb{Z})^{\times}$ of size m. Set $\omega = e^{\frac{2\pi i}{n}}$, $\mathbf{v} = \frac{1}{\sqrt{m}}[1, ..., 1]^T \in \mathbb{R}^m$, and $\mathbf{U} = \text{diag}(\omega^{a_1}, ..., \omega^{a_m})$. Then the inner products between the vectors $\{\mathbf{U}^\ell \mathbf{v}\}_{\ell=0}^{n-1}$ take on only $\frac{n-1}{m}$ values (possibly non-unique), each value occurring with the same number of times as one of these mutual inner products.

Proof: This proof appears in [37]. The idea is that the inner product corresponding to the element $\mathbf{U}^\ell$ in (7) is

$$\mathbf{v}^* \mathbf{U}^\ell \mathbf{v} = \sum_{i=1}^{n} \omega^{\ell a_i}, \tag{10}$$

and we can see that this sum depends only on the *coset* of A in which ℓ lies in the group $(\mathbb{Z}/n\mathbb{Z})^{\times}$. There is only one inner product value for each of the $\frac{n-1}{m}$ cosets, and it is not too difficult to see that each of these values arises the same number of times as an inner product $\mathbf{v}^* \mathbf{U}^{-\ell_1} \mathbf{U}^{\ell_2} \mathbf{v}$ between two frame vectors $\mathbf{U}^{\ell_1} \mathbf{v}$ and $\mathbf{U}^{\ell_2} \mathbf{v}$. ■

Figure 1 depicts how choosing the exponents in (9) according to Theorem 2 reduces the number of distinct inner product values and yields low coherence frames. This theorem allows us to bound the coherence of our frames using Lemma 2, but it turns out that we can achieve even tighter bounds by exploiting the algebraic structure employed in constructing our frames. In [36], we presented the following bounds:

Theorem 3 (General κ): Let n be a prime, m a divisor of $n-1$, and $\omega = e^{\frac{2\pi i}{n}}$. Let $A = \{a_1, ..., a_m\}$ be the unique subgroup of $(\mathbb{Z}/n\mathbb{Z})^{\times}$ of size m, and set $\mathbf{U} = diag(\omega^{a_1}, ..., \omega^{a_m}) \in \mathbb{C}^{m \times m}$, $\mathbf{v} = \frac{1}{\sqrt{m}}[1, ..., 1]^T \in \mathbb{C}^{m \times 1}$, and $\mathbf{M} = [\mathbf{v}, \mathbf{U}\mathbf{v}, ..., \mathbf{U}^{n-1}\mathbf{v}]$.

If $\kappa := \frac{n-1}{m}$, then the coherence μ of $\mathbf{M}$ satisfies the following upper bound:

$$\mu \leq \frac{1}{\kappa} \left((\kappa - 1) \sqrt{\frac{1}{m} \left(\kappa + \frac{1}{m} \right) + \frac{1}{m}} \right). \tag{11}$$

Proof: We will actually realize this result in a slightly more general context, and will prove it in Appendix A. ■

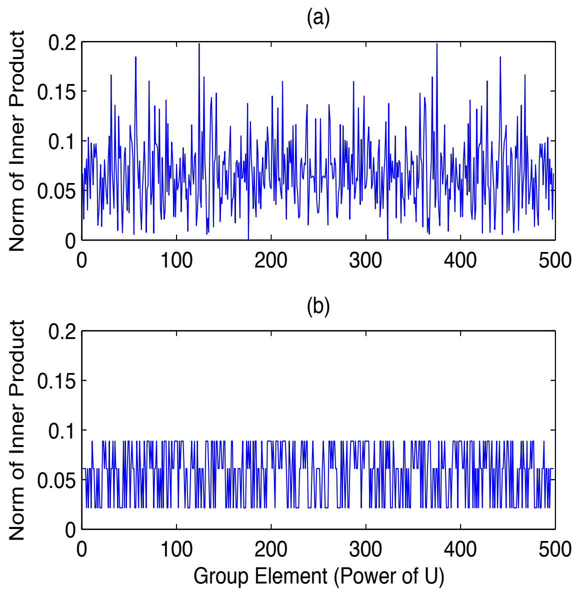


Figure 1: The norms of the inner products between the frame elements of $\mathbf{M}$ in (9). Here, $n = 499$ and $m = 166$. There is one inner product for each element U^ℓ of the cyclic group $\langle U \rangle \cong (\mathbb{Z}/n\mathbb{Z})^\times$, where n is prime. (a) The exponents $A = \{a_i\}_{i=1}^m$ in (9) are chosen randomly. (b) A is chosen to be the unique subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ of index 3. In this case, there are only 3 distinct inner product norms—one for each coset of A—each arising the same number of times. This leads to lower coherence.

Interestingly, we can find an even tighter bound for the coherence of our frames in the case when m is odd:

Theorem 4 (m odd): Let n be an odd prime, m a divisor of $n-1$, and $\omega = e^{\frac{2\pi i}{n}}$. Let $A = \{a_1, ..., a_m\}$ be the unique subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ of size m, and set $\mathbf{U} = \mathrm{diag}(\omega^{a_1}, ..., \omega^{a_m}) \in \mathbb{C}^{m\times m}$, $\mathbf{v} = \frac{1}{\sqrt{m}}[1, ..., 1]^T \in \mathbb{C}^{m\times 1}$, and $\mathbf{M} = [\mathbf{v}, \mathbf{U}\mathbf{v}, ..., \mathbf{U}^{n-1}\mathbf{v}]$. Set $\kappa := \frac{n-1}{m}$.

If m is odd, then the coherence of $\mathbf{M}$ is upper-bounded by

$$\mu \leq \frac{1}{\kappa}\sqrt{\left(\frac{1}{m} + \left(\frac{\kappa}{2} - 1\right)\beta\right)^2 + \left(\frac{\kappa}{2}\right)^2 \beta^2}, \tag{12}$$

where $\beta = \sqrt{\frac{1}{m}\left(\kappa + \frac{1}{m}\right)}$.

Proof: This is proved in Appendix A. ■

It turns out that we can realize our method of constructing frames from cyclic groups in a much more general context, which we will detail in the upcoming sections. While Theorems 3 and 4 will only generalize in certain scenarios, we will always be able to use Lemma 2 to bound our frames' coherence.

III. Tight Group Frames and the Group Fourier Matrix

In light of Lemmas 1 and 2, we will first establish the tools we need to ensure that our group frames are tight. It turns out that the tight group frames have been completely classified [10], [42]. On this note, we review some basics on representation theory, which the interested reader can read about in greater depth in the first few chapters of [30].

Let G be a group of size n, and recall that a complex representation of G is formally defined as a complex vector space V together with a function $\rho : G \to GL(V)$ such that $\rho(gg') = \rho(g)\rho(g')$, $\forall g, g' \in G$. If V has dimension d, then $\rho(g)$ is simply a $d \times d$ invertible complex matrix—a *degree* d representation. Two representations ρ_1 and ρ_2 with corresponding vector spaces V_1 and V_2 are *equivalent* if there is an invertible transformation $T : V_1 \to V_2$ such that $T\rho_1(g)T^{-1} = \rho_2(g)$ for all $g \in G$. A basic result in representation theory says that every representation of a finite group is equivalent to a unitary representation, in which all the $\rho(g_i)$ are unitary matrices, which is why we have used the notation $\rho(g_i) = \mathbf{U}_i$ in our previous discussion. We will typically assume our representations are unitary without loss of generality.

A representation ρ is *reducible* if there is a nontrivial subspace V' of V which is mapped to itself by $\rho(g)$ for every $g \in G$. Otherwise, it is called *irreducible*. As matrices, the representation is reducible if the $\rho(g)$ can be simultaneously block-diagonalized by a similarity transformation. For any finite group G of size n, there are only a finite number of inequivalent, irreducible unitary representations. If we call them ρ_1, ..., ρ_{n_r} with corresponding degrees $d_1, ..., d_{n_r}$, then it can be shown [30] that these degrees satisfy the relation

$$\sum_{i=1}^{n_r} d_i^2 = |G|. \tag{13}$$

Every complex representation of G is equivalent to an orthogonal direct sum of irreducible representations. Formally, this means that there is an invertible linear transformation $T : V \to V_1 \oplus ... \oplus V_m$ such that the V_i are mutually orthogonal vector spaces and $T\rho(g)T^{-1} = \rho_1(g) \oplus ... \oplus \rho_m(g)$, where for each i, ρ_i and V_i give an irreducible representation of G. These irreducible representations can again be taken to be unitary. As matrices, this means that the $\rho(g)$ can be simultaneously block-diagonalized in the form $\rho(g) = \mathrm{diag}(\rho_1(g), ..., \rho_m(g))$. A basic result of representation theory is that this decomposition into irreducible components is unique up to isomorphism. We are now ready to give a classification of all the tight G-frames:

Theorem 5 ([10]): Let $G = \{g_i\}_{i=1}^n$ be a finite group, and $\rho : G \to GL(V)$ a complex representation of G which has the decomposition into orthogonal unitary irreducible representations:

$$V = V_1 \oplus ... \oplus V_m,$$

$$\rho(g) = \rho_1(g) \oplus ... \oplus \rho_m(g).$$

Let $\mathbf{v} = \mathbf{v}_1 + ... + \mathbf{v}_m$, $\mathbf{v}_k \in V_k$, and set $\mathbf{f}_i = \rho(g_i)\mathbf{v}$. Then $\{\mathbf{f}_i\}_{i=1}^n$ is a tight G-frame if and only if

- $\frac{||\mathbf{v}_i||_2^2}{||\mathbf{v}_j||_2^2} = \frac{\dim(V_i)}{\dim(V_j)}$, and
- if the i^{th} and j^{th} irreducible components are equivalent via $T : V_i \to V_j$, then $T\mathbf{v}_i$ and $\mathbf{v}_j$ are orthogonal.

Proof: This is Theorem 5.4 in [10]. It follows from considering the frame matrix $\mathbf{M} := \begin{bmatrix} \dots & \rho(g_i)\mathbf{v} & \dots \end{bmatrix}_{i=1}^n$ and applying Schur's Lemma (Section 2.2, [30]) to the product $\mathbf{M}\mathbf{M}^*$ to see when it is a scalar matrix, which is equivalent to the columns of $\mathbf{M}$ forming a tight frame. ■

We will now establish a tool that will allow us to easily use this theorem to construct tight frames. On this note, consider the following well-studied generalization of the classical discrete Fourier transform [34]:

Definition 2: We define the *group Fourier transform* of a complex-valued function on G, $f : G \to \mathbb{C}$, to be the function that maps a degree d representation ρ to the $d \times d$ complex matrix

$$\hat{f}(\rho) = \sum_{g \in G} f(g)\rho(g). \tag{14}$$

There is an inverse transformation given by

$$f(g) = \frac{1}{|G|} \sum_{i=1}^{n_r} d_i \mathrm{Tr}(\rho_i(g^{-1})\hat{f}(\rho_i)), \tag{15}$$

where the sum is taken over all the inequivalent irreducible representations of G.

Much like the traditional discrete Fourier transform, this transformation has a matrix representation in the form

$$\mathcal{F} = \begin{bmatrix} \sqrt{d_1}\mathrm{vec}(\rho_1(g_1)) & \dots & \sqrt{d_1}\mathrm{vec}(\rho_1(g_n)) \\ \sqrt{d_2}\mathrm{vec}(\rho_2(g_1)) & \dots & \sqrt{d_2}\mathrm{vec}(\rho_2(g_n)) \\ \vdots & \ddots & \vdots \\ \sqrt{d_{n_r}}\mathrm{vec}(\rho_{n_r}(g_1)) & \dots & \sqrt{d_{n_r}}\mathrm{vec}(\rho_{n_r}(g_n)) \end{bmatrix}, \tag{16}$$

where for a $d \times d$ matrix A, vex(A) is the *vectorization* of A, i.e., the vector formed by stacking the columns of A into a single $d^2 \times 1$ column. From equation (13), we see that $\mathcal{F}$ is a square matrix.

Notice that when G is a cyclic group of size n, then the group elements are $\{0, 1, ..., n-1\}$ (with the group operation being addition modulo n). Since this group is abelian, there are exactly n irreducible representations, $\{\rho_\ell\}_{\ell=1}^{n}$, each degree-1. ρ_ℓ is simply the function that maps $k \mapsto \omega^{k\ell}$, $k \in \{0, ..., n-1\}$, where $\omega = e^{\frac{2\pi i}{n}}$. In this case our group Fourier transform and matrix become the familiar discrete time Fourier transform and DFT matrix.

Theorem 6: Let $G = \{g_i\}_{i=1}^{n}$ be a finite group with inequivalent, irreducible representations $\{\rho_i\}_{i=1}^{n_r}$, and $\mathcal{F}$ the group Fourier matrix of G as in (16). Then the columns of $\mathcal{F}$ form a tight G-frame, so $\mathcal{F}$ is a unitary matrix. In fact, if $\tilde{\rho} : G \to \mathbb{C}^{d\times d}$ is a representation of G and $\tilde{\mathbf{v}} \in \mathbb{C}^{d\times 1}$ such that the columns of $\mathbf{M} := [\dots \ \tilde{\rho}(g_i)\tilde{\mathbf{v}} \ \dots]_{i=1}^{n}$ form a tight frame, then the rows of $\mathbf{M}$ are a subset of the rows of $\mathcal{F}$ up to an equivalence of $\tilde{\rho}$ or a change of basis of $\mathbb{C}^{d\times 1}$.

Proof: The group Fourier matrix $\mathcal{F}$ can be realized as a G-frame as follows: For each $i = 1, ..., n_r$, define the representation

$$\tilde{\rho}_i(g) = \mathrm{diag}(\rho_i(g), ..., \rho_i(g)) \in \mathbb{C}^{d_i^2 \times d_i^2}, \tag{17}$$

a direct sum of d_i copies of the irreducible representation ρ_i. Also define the vector

$$\mathbf{v}_i = \mathrm{vec}(\mathbf{I}_{d_i}) = [\mathbf{e}_i^{(1)T}, ..., \mathbf{e}_i^{(d_i)T}]^T \in \mathbb{C}^{d_i^2}, \tag{18}$$

where $\mathbf{I}_{d_i}$ is the $d_i \times d_i$ identity matrix and $\mathbf{e}_i^{(j)} \in \mathbb{C}^{d_i\times 1}$ is the j^{th} column of $\mathbf{I}_{d_i}$—a vector of all zeros except for a 1 in the j^{th} position.

Now choose the representation

$$\rho(g) = \mathrm{diag}(\tilde{\rho}_1(g), \tilde{\rho}_2(g), ..., \tilde{\rho}_{n_r}(g)) \in \mathbb{C}^{n\times n}, \tag{19}$$

and the vector

$$\mathbf{v} = [\sqrt{d_1}\mathbf{v}_1^T, \sqrt{d_2}\mathbf{v}_2^T, \ldots, \sqrt{d_{n_r}}\mathbf{v}_{n_r}^T]^T \in \mathbb{C}^n. \tag{20}$$

Then $\mathcal{F}$ is the G-frame with columns $\rho(g_i)\mathbf{v}$. For any i, $\{\mathbf{e}_i^{(j)}\}_{j=1}^{d_i}$ is a complete orthonormal set in $\mathbb{C}^{d_i}$, and $\frac{||e_{i_1}^{(j_1)}||_2^2}{||e_{i_2}^{(j_2)}||_2^2} = \frac{d_{i_1}}{d_{i_2}}$. From Theorem 5, we see that not only do the columns of $\mathcal{F}$ form a tight G-frame, but in fact up to a change of basis of the $\mathbf{e}_i^{(j)}$ or a similarity transformation of the ρ_i, every tight G-frame can be realized as a subset of the rows of $\mathcal{F}$ by forming each $\mathbf{v}_i$ from a corresponding *subset* of the columns $\{\mathbf{e}_i^{(j)}\}_{j=1}^{d_i}$. ∎

Theorem 6 reduces the task of constructing tight G-frames to selecting blocks of rows of the corresponding group Fourier matrix $\mathcal{F}$. Our job will now be to find good choices of the group G, and to identify which rows of $\mathcal{F}$ to choose to create a tight group frame with low coherence. We should mention that this problem was explored for abelian groups G in [16], with a focus on finding frames with coherence equal to the Welch Bound. We will find, however, that by not placing any restrictions on our group G, and by allowing our coherence to be slightly above the Welch lower bound, we can produce a vastly larger and richer collection of frames.

IV. Reducing the Number of Distinct Inner Products in Tight Group Frames

In our original construction from Theorem 2, we designed harmonic frames in the form of $\mathbf{M}$ from (9) which arose from representations of the cyclic group $G = \mathbb{Z}/n\mathbb{Z}$, where n is a prime. Indeed, the j^{th} row of $\mathbf{M}$ is $[1, \omega^{k_j}, \omega^{2k_j}, ..., \omega^{(n-1)k_j}$, where $\omega = e^{\frac{2\pi i}{n}}$, and we can now see that this is simply the row of the group Fourier matrix of G corresponding to the n-dimensional representation $\rho_{k_j}(\ell) = \omega^{\ell k_j}$, for $\ell \in \{0, ..., n-1\}$. We wish to generalize our original method from Theorem 2 of constructing frames with few distinct inner product values.

On this note, we will consider constructing frames by choosing the blocks of rows corresponding to m of the representations, which we may assume are $\rho_1, ..., \rho_m$ up to a reordering, so that our frame matrix takes the form

$$\mathbf{M} = \begin{bmatrix} \sqrt{d_1}\mathrm{vec}(\rho_1(g_1)) & \dots & \sqrt{d_1}\mathrm{vec}(\rho_1(g_n)) \\ \vdots & \ddots & \vdots \\ \sqrt{d_m}\mathrm{vec}(\rho_m(g_1)) & \dots & \sqrt{d_m}\mathrm{vec}(\rho_m(g_n)) \end{bmatrix}. \tag{21}$$

As an analog to Equations (19) and (20) from the proof of Theorem 6, this corresponds to the tight group frame whose elements are the images of the vector $\mathbf{v} = [\sqrt{d_1}\mathbf{v}_1^T, \sqrt{d_2}\mathbf{v}_2^T, \dots, \sqrt{d_m}\mathbf{v}_m^T]^T$ under the representation $\rho(g) = \mathrm{diag}(\tilde{\rho}_1(g), \tilde{\rho}_2(g), ..., \tilde{\rho}_m(g))$, where $\tilde{\rho}_i$ and $\mathbf{v}_i$ are defined as in Equations (17) and (18) respectively. The dimension of this representation is easily seen to be $\sum_{i=1}^m d_i^2$. Note that in the setting of Theorem 2, the representations ρ_i are all 1-dimensional, so the block $\begin{bmatrix}\sqrt{d_i}\mathrm{vec}(\rho_i(g_1)) & \dots & \sqrt{d_i}\mathrm{vec}(\rho_i(g_n))\end{bmatrix}$ is just a single row.

The inner product between the i^{th} and j^{th} columns of $\mathbf{M}$ in (21) takes the form

$$\sum_{t=1}^m d_t \mathrm{vec}(\rho_t(g_i))^* \mathrm{vec}(\rho_t(g_j)) = \sum_{t=1}^m d_t \mathrm{Tr}(\rho_t(g_i)^* \rho_t(g_j)) \tag{22}$$

$$= \sum_{t=1}^m d_t \mathrm{Tr}(\rho_t(g_i^{-1} g_j)) \tag{23}$$

$$= \sum_{t=1}^m d_t \chi_t(g_i^{-1} g_j). \tag{24}$$

Here, $\chi_i(g) := \mathrm{Tr}(\rho_i(g))$ is the *character function* associated to the representation ρ_i. Equation (24) actually arises in [16], though only 1-dimensional representations are considered, in which case each representation is essentially just its own character. Note that in this form the frame is unnormalized, but all of the columns have the same norm, which is given by the square root of the inner product associated to the identity element:

$$||\rho(g)\mathbf{v}||_2 = \sqrt{\sum_{t=1}^m d_t \chi_t(1)} = \sqrt{\sum_{t=1}^m d_t^2}, \tag{25}$$

where we have used the fact the character evaluated at 1 is simply the dimension of the representation. Alternatively, we could have simply seen this to be the norm of $\mathbf{v}$ by speculation.

Basic representation theory tells us that a character χ completely determines its representation up to isomorphism, and as such the characters of many groups are well-studied. In light of this fact, we can often compute the coherence of frames in the form of (21) for different choices of representations $\{\rho_i\}_{i=1}^m$ without explicitly building the frame matrix $\mathbf{M}$, which can often be a tedious computation. From (23) and (24) we see that the inner product depends only on the group element $g_k := g_i^{-1}g_j$, so a priori there are only $n-1$ possible nontrivial distinct inner product values, and each of these values arises the same number of times as the inner product between two columns. This was to be expected, since the columns of $\mathbf{M}$ form a group frame in light of Theorem 6. If we could generalize our method for choosing rows of the classical Fourier matrix, however, we could hope to reduce this number even further.

Toward this end, we consider the group of *automorphisms* of G. An automorphism of G is a bijective function $\sigma : G \to G$ which respects the group multiplication, i.e. $\sigma(gg') = \sigma(g)\sigma(g')$ for any $g, g' \in G$. The automorphisms of G form a group under composition, denoted $Aut(G)$. An important subgroup of $Aut(G)$ is that of the *inner automorphisms*, denoted $Inn(G)$. These are the automorphisms which arise from *conjugation* by an element $h \in G$, which is the function $\sigma_h(g) = hgh^{-1}$. Two elements g and g' are said to be *conjugate* if there is some $h \in G$ such that $g' = hgh^{-1}$, and the set of all elements conjugate to g is called the *conjugacy class* $\mathcal{C}_g$. We see that the relation $\{g \sim g' \iff g \text{ is conjugate to } g'\}$ is an equivalence relation on G, so G can be partitioned into a disjoint union of its conjugacy classes. $Inn(G)$ is easily verified to be a normal subgroup of $Aut(G)$, and the quotient group $Aut(G)/Inn(G)$ is called the group of *outer automorphisms*, denoted $Out(G)$.

Any conjugation $\sigma_h \in Inn(G)$ fixes a representation's character function. Indeed, if ρ is a representation of G with associated character χ, then

$$\chi(\sigma_h(g)) = \chi(hgh^{-1}) = \mathrm{Tr}(\rho(h)\rho(g)\rho(h)^{-1}) = \mathrm{Tr}(\rho(g)) = \chi(g). \tag{26}$$

Thus, since the inner products between the columns of $\mathbf{M}$ in (21) can be expressed as in (24) in terms of the characters of the irreducible representations of G (i.e. a so-called *character function* on the group elements), we see that there is really only one inner product value for each conjugacy class of G. Note that while this observation has the advantage of reducing the number of distinct inner product values to consider, we unfortunately cannot readily apply Lemma 2 to obtain a tighter coherence bound since these values no longer occur with the same multiplicity. Indeed, for each $g \in G$, the corresponding inner product value $\sum_{t=1}^m d_t\chi_t(g)$ will arise once for each element in the conjugacy class $\mathcal{C}_g$, and the conjugacy classes need not have the same size.

Since an automorphism essentially preserves the structure of the group G, it is no surprise that it also preserves the structure of its representations:

Lemma 4: $\rho(g)$ is an irreducible representation of the finite group G if and only if $\rho(\sigma(g))$ is also an irreducible representation for any $\sigma \in Aut(G)$. Furthermore, $\rho(g)$ and $\rho(\sigma(g))$ have the same degrees.

Proof: If $\rho : G \to GL(V)$ is a representation, then composing with the automorphism $\sigma : G \to G$ yields a function $\rho \circ \sigma : G \to GL(V)$ which respects the group multiplication: $\rho(\sigma(gg')) = \rho(\sigma(g)\sigma(g')) = \rho(\sigma(g))\rho(\sigma(g'))$. Thus, $\rho(\sigma(g))$ is a well-defined representation which clearly has the same dimension as $\rho(g)$. Furthermore, since σ is a bijection of G, the matrices $\{\rho(\sigma(g)) \ : \ g \in G\}$ are simply a permutation of the matrices $\{\rho(g) \ : \ g \in G\}$, so the first representation is irreducible if and only if the second is. ■

If ρ is a representation with character χ, and $\sigma \in Aut(G)$, we will use the notation ρ_σ to indicate the representation

$$\rho_\sigma(g) := \rho(\sigma(g)), \tag{27}$$

which is irreducible if ρ is. ρ_σ has corresponding character

$$\chi_\sigma(g) := \chi(\sigma(g)). \tag{28}$$

Under this notation, if $\mathbf{1} \in Aut(G)$ denotes the identity automorphism $\mathbf{1}(g) = g$, then $\rho_{\mathbf{1}}$ and $\chi_{\mathbf{1}}$ are simply ρ and χ respectively. From Lemma 4, we see that $Aut(G)$ has a group action on the irreducible representations and characters of G given by

$$\sigma' \cdot \rho_\sigma := \rho_{\sigma\sigma'}, \tag{29}$$

$$\sigma' \cdot \chi_\sigma := \chi_{\sigma\sigma'}. \tag{30}$$

Let us consider case in our original construction from Theorem 2 where G was the (additive) cyclic group $\mathbb{Z}/n\mathbb{Z} = \{0, ..., n-1\}$. In this case, $Aut(G)$ is isomorphic to the (multiplicative) group of elements relatively prime to n, $(\mathbb{Z}/n\mathbb{Z})^\times$. For each $\ell \in (\mathbb{Z}/n\mathbb{Z})^\times$, the corresponding automorphism $\sigma_\ell \in Aut(G)$ is given by $\sigma_\ell(g) = \ell g$. When we required that n be prime in Theorem 2, we ensured that every nonzero element had a multiplicative inverse modulo n, so in this case $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set $\{1, ..., n-1\}$.

Refer back to the structure of our harmonic frame from (9):

$$\mathbf{M} = \frac{1}{\sqrt{m}} \begin{bmatrix} 1 & \omega^{a_1} & \omega^{a_1 \cdot 2} & \dots & \omega^{a_1 \cdot (n-1)} \\ 1 & \omega^{a_2} & \omega^{a_2 \cdot 2} & \dots & \omega^{a_2 \cdot (n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{a_m} & \omega^{a_m \cdot 2} & \dots & \omega^{a_m \cdot (n-1)} \end{bmatrix}, \tag{31}$$

where $\omega = e^{2\pi i/n}$. As we have discussed, selecting the frequencies $\{a_1, ..., a_m\}$ is equivalent to choosing rows of the group Fourier matrix corresponding to $\mathbb{Z}/n\mathbb{Z}$, each of which corresponds to a degree-1 representation. By choosing the frequencies $\{a_1, ..., a_m\}$ in (31) to be a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ as in Theorem 2, we can now see that we are actually choosing a subgroup of $Aut(G)$. Without loss of generality, let $a_1 = 1$ so that the first row of (31) corresponds to the representation $\rho(g) = \omega^g$. Then the i^{th} row corresponds to the representation $\rho_i(g) := \rho(\sigma_{a_i}(g)) = \omega^{a_i g}$. Thus, we have formed $\mathbf{M}$ by choosing the rows of the group Fourier matrix corresponding to a subset of representations of the form $\{\sigma_i \cdot \rho\}$, where the $\{\sigma_i\}$ form a subgroup of automorphisms.

We wish to generalize this process to groups G other than $\mathbb{Z}/n\mathbb{Z}$ by choosing an irreducible representation ρ of G and taking its image under a subgroup of automorphisms $\{\sigma_i\} \leq Aut(G)$. Note that from Lemma 4, the representations $\{\sigma_i \cdot \rho\}$ will all be irreducible, and hence correspond to easily-identified blocks of rows from the group Fourier matrix $\mathcal{F}$ in (16). It is not clear, however, whether these representations will be distinct. The question now becomes how to choose the subgroup of automorphisms?

V. Choosing the Automorphism Subgroup

Let $H \leq Aut(G)$ be a group of automorphisms of G, and fix an irreducible representation ρ with character χ. Define K to be the subgroup of H which fixes χ:

$$K = \{\sigma \in H \ : \ \chi(\sigma(g)) = \chi(g), \ \forall g \in G\}. \tag{32}$$

Immediately we see that K contains every inner automorphism in H. Thus, it is effectively the group of *outer* automorphisms which acts nontrivially on the representations. Now choose a subgroup $A \leq H$ such that the group product $KA := \{ka \ : \ k \in K, \ a \in A\}$ is a subgroup of H. This is equivalent to the group products KA and AK being equal as sets. We consider choosing the rows of the generalized Fourier matrix corresponding to the representations

$\{\rho_a \ : \ a \in A\}$, with notation as in (27). From Lemma 4, all of these representations have the same degree d. Thus, if $A = \{a_1, ..., a_m\} \leq Aut(G)$, then $\mathbf{M}$ takes the form

$$\mathbf{M} = \sqrt{d} \begin{bmatrix} \mathrm{vec}(\rho_{a_1}(g_1)) & \dots & \mathrm{vec}(\rho_{a_1}(g_n)) \\ \vdots & \ddots & \vdots \\ \mathrm{vec}(\rho_{a_m}(g_1)) & \dots & \mathrm{vec}(\rho_{a_m}(g_n)) \end{bmatrix}. \tag{33}$$

Notice that if A and K have nontrivial intersection, then some of the blocks of rows of $\mathbf{M}$ above may correspond to repeated or isomorphic representations. If this is the case our frame will no longer be tight. We can avoid this by assuming that $|K \cap A| = 1$, though we will typically not make use of this assumption in our following proofs.

Now let us examine the inner products between our frame elements. From (24), the inner product corresponding to the group element g is

$$d \sum_{a \in A} \chi_a(g) = d \sum_{a \in A} \chi(a(g)). \tag{34}$$

Our aim is to generalize the concept from Theorem 2 of having one inner product per coset of a subgroup of $Aut(G)$. We first establish the following preliminary lemma:

Lemma 5: Let A and K be subgroups of a finite group H such that the set product KA is a group, and let $\{a_i\}_{i=1}^{|A|/|A \cap K|}$ be a set of right coset representatives for $(A \cap K) \backslash A$. Then for each fixed a_i and $k \in K$, there is a unique $a_{i'}$ and $k' \in K$ such that $a_{i'} k = k' a_i$, and a unique $a_{i''}$ and $k'' \in K$ such that $a_i k = k'' a_{i''}$.

Proof: Since KA is a group (by assumption) which obviously contains both K and A, we can write $a_i k = \tilde{k}\tilde{a}$ for some $\tilde{k} \in K$ and $\tilde{a} \in A$. Then $\tilde{a}$ can further be written uniquely in the form $\tilde{k}_2 a_{i''}$ for some $\tilde{k}_2 \in A \cap K$ and $a_{i''}$ one of the right coset representatives of $A \cap K$ in A. Setting $k'' = \tilde{k}\tilde{k}_2$ gives us the second part of this theorem.

Now suppose there are two pairs (a_j, k'_j) and (a_t, k'_t) such that

$$a_j k = k'_j a_i, \tag{35}$$

$$a_t k = k'_t a_i. \tag{36}$$

Then from (36) we have $a_t (a_j)^{-1} a_j k = k'_t (k'_j)^{-1} k'_j a_i$, and we can use (35) to cancel out $a_j k$ and $k'_j a_i$ from this expression to arrive at

$$a_t (a_j)^{-1} = k'_t (k'_j)^{-1} \in A \cap K. \tag{37}$$

But since a_t and a_j are representatives of distinct right cosets of $A \cap K$ in A, they must be equal, hence $a_t = a_j$ and $k'_t = k'_j$. This shows that there can only be *at most* one pair $(a_{i'}, k')$ such that $a_{i'}k = k'a_i$. But since we have already shown that every a_jk can be written uniquely in the form $k''a_{j''}$ for some $a_{j''}$, then since our groups are finite there must be some j for which $a_{j''} = a_i$, so there is *exactly* one such pair $(a_{i'}, k') = (a_j, k'')$ which satisfy the hypotheses of the lemma. ■

The next lemma now extends the coset idea of Theorem 2 to drastically reduce the number of distinct inner product values we need consider.

Lemma 6: Let G be a finite group, $H \leq Aut(G)$, ρ an irreducible representation of G with character χ, and K the subgroup of H which fixes χ as in (32). Let A be a subgroup of H such that KA is a group. Then for any $\sigma_1, \sigma_2 \in H$ which are in the same *right* coset of KA, the inner products associated to $\sigma_1(g)$ and $\sigma_2(g)$ respectively are equal for any $g \in G$. That is,

$$d \sum_{a \in A} \chi_a(\sigma_1(g)) = d \sum_{a \in A} \chi_a(\sigma_2(g)). \tag{38}$$

Proof: Since σ_1 and σ_2 are in the same right coset of KA (which is equal to AK), there is some $h \in H$ such that $\sigma_1 = a_1k_1h$ and $\sigma_2 = a_2k_2h$ for some $a_1, a_2 \in A$ and some $k_1, k_2 \in K$. Thus, (34) becomes

$$d \sum_{a \in A} \chi(a\sigma_1(g)) = d \sum_{a \in A} \chi(aa_1k_1h(g)) \tag{39}$$

$$= d \sum_{a \in A} \chi(ak_1h(g)), \tag{40}$$

which follows from the fact that multiplication by a_1 permutes the elements of A.

Now let $\{a_i\}$ be a set of right coset representatives for $(A \cap K)\backslash A$. Our sum now becomes

$$d \sum_{a \in A} \chi(ak_1h(g)) = d \sum_{a_i} \sum_{\gamma \in A \cap K} \chi(\gamma a_ik_1h(g)) \tag{41}$$

$$= d \sum_{a_i} |A \cap K| \chi(a_ik_1h(g)), \tag{42}$$

which follows from fact that elements of K fix χ. Now for each a_i, we know from Lemma 5 that a_ik_1 is uniquely expressible in the form k'_ja_j for some right coset representative a_j and some $k'_j \in K$. Thus, since the $\{a_i\}$ and $\{a_j\}$ are in one to one correspondence by Lemma 5, we can further rewrite our sum as

$$d\sum_{a_i} |A\cap K|\chi(a_i k_1 h(g)) = d\sum_{a_j} |A\cap K|\chi(k'_j a_j h(g)) \tag{43}$$

$$= d\sum_{a_j} |A\cap K|\chi(a_j h(g)) \tag{44}$$

$$= d\sum_{a_j} \sum_{\gamma\in A\cap K} \chi(\gamma a_j h(g)) \tag{45}$$

$$= d\sum_{a\in A} \chi(ah(g)). \tag{46}$$

Since the inner product depends only on h, we are done. ■

We can now express each inner product in terms of a right coset of KA and an *orbit* of G under the automorphism group H. Two elements $g, g' \in G$ are said to be in the same orbit if there is an automorphism $h \in H$ such that $h(g) = g'$. Note that since $g = h^{-1}(g')$, this is an equivalence relation, so the orbits partition G. We may write this orbit as $Hg := \{h(g) \mid h \in H\}$, and we say that g is a *representative* of this orbit. It should be clear that the identity element $1 \in G$ is in its own orbit.

We are now equipped to bound both the number of distinct inner product values, as well as the coherence of our new frames. The following theorem contains the analogs of Lemma 2 and Theorem 2 to the broader class of frames we have just constructed.

Theorem 7: Let G be a finite group of size n and ρ a degree-d irreducible representation of G with character χ. Define

- $H \leq Aut(G)$ a group of automorphisms of G,
- $K := \{\sigma \in H \ : \ \chi(\sigma(g)) = \chi(g), \ \forall g \in G\}$, the subgroup of H consisting of automorphisms which fix χ,
- $A = \{a_i\}_{i=1}^m \leq H$, any subgroup of H such that the set product KA is also subgroup of H with $A \cap K = 1$,
- $\{h_i\}_{i=1}^{n_c}$ representatives of the distinct cosets of KA in H
- $\{g_j\}_{j=1}^{n_o}$ representatives of the distinct orbits of G under H

Finally, let $\mathbf{M}$ be the frame with elements $\{\sqrt{d}[\text{vec}(\rho_{a_1}(g))^T, ..., \text{vec}(\rho_{a_m}(g))^T]^T\}_{g\in G}$ as in (33). Then $\mathbf{M}$ is a tight frame with at most $n_c(n_o - 1)$ distinct inner product values between its vectors. If μ_W is the lower bound on coherence given by the Welch bound (explicitly $\mu_W = \sqrt{\frac{n-dm}{dm(n-1)}}$), then the coherence μ of our frame is bounded by

$$\mu \leq \sqrt{\frac{|G|-1}{\min_{\{(i,j):g_j\neq 1\}} |KAh_i(g_j)|}}\mu_W. \tag{47}$$

Proof: By hypothesis, G is partitioned into distinct orbits $Hg_1, ..., Hg_{n_o}$ with representatives $g_1, ..., g_{n_o}$. Let $g \in G$ be in the j^{th} orbit so that for some $h \in H$ we have $h(g_j) = g$. Suppose that $h \in KAh_i$. Then from Lemma 6, the inner product associated to g is

$$d\sum_{a\in A}\chi(a(g)) = d\sum_{a\in A}\chi(ah(g_j)) = d\sum_{a\in A}\chi(ah_i(g_j)). \tag{48}$$

Thus, excluding the orbit corresponding to the identity element (which corresponds to taking the inner product of a column of $\mathbf{M}$ with itself), the number of nontrivial inner products that we must consider is $n_c(n_o - 1)$, and the number of times the inner product corresponding to the pair (h_i, g_j) arises is

$$|KAh_i(g_j)| = \#\{kah_i(g_j) \ : \ k \in K, \ a \in A\}. \tag{49}$$

Now since our frame $\mathbf{M}$ is tight by Theorem 6, then from Lemma 2, the mean squared inner product between the frame vectors is equal to μ_W^2, and this mean can be written as

$$\mu_W^2 = \frac{1}{\sum_{h_i}\sum_{g_j\neq 1}|KAh_i(g_j)|}\cdot\sum_{h_i}\sum_{g_j\neq 1}|KAh_i(g_j)||\alpha_{i,j}|^2 \tag{50}$$

$$= \frac{1}{|G|-1}\cdot\sum_{h_i}\sum_{g_j\neq 1}|KAh_i(g_j)||\alpha_{i,j}|^2, \tag{51}$$

where $\alpha_{i,j}$ is the inner product associated to the pair (h_i, g_j). From this, it follows that

$$(|G|-1)\mu_W^2 \geq \left(\min_{\{(i,j):g_j\neq 1\}} |KAh_i(g_j)|\right)\left(\max_{\{(i,j):g_j\neq 1\}} |\alpha_{i,j}|^2\right),$$

from which our result follows.

■

We can see from Theorem 7 that in general our coherence will be closer to the Welch bound if we have fewer orbits, and the sets $KAh_i(g_j)$ are close to each other in size. We articulate this in the following corollary.

Corollary 1: In Theorem 7, if the sets $KAh_i(g_j)$ are the same size for all h_i and all nonidentity g_j, we achieve our optimal upper bound in (47):

$$\mu \leq \sqrt{n_c(n_o-1)}\mu_W. \tag{52}$$

Proof: If there are n_c cosets of KA in H, and n_o orbits of G under the action of H, then since $\sum_{h_i}\sum_{g_j\neq 1}|KAh_i(g_j)| = |G|-1$, we have

$$\min_{\{(i,j):g_j\neq 1\}} |KAh_i(g_j)| \leq \frac{|G|-1}{n_c(n_o-1)}, \tag{53}$$

with equality if and only if the sets $KAh_i(g_j)$ are all the same size. The result follows immediately. ■

For clarity, let us reiterate how our frames from Theorem 2 fall into the more general framework of Theorem 7. In this case,

- G is the cyclic additive group $\mathbb{Z}/n\mathbb{Z} = \{0,1,...,n-1\} \mod n$, where n is a prime.
- ρ is the representation $\rho(x) = e^{\frac{2\pi ix}{n}}$ for any $x \in G$.
- $\chi(x)$ is equal to $\rho(x)$ for any $x \in G$, since ρ is a degree-1 representation.
- H is the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times = \{1,2,...,n-1\} \mod n$, where each element $h \in (\mathbb{Z}/n\mathbb{Z})^\times$ is viewed as an automorphism $h(x) = h \cdot x$.
- K is the subgroup of H such that $e^{\frac{2\pi ikx}{n}} = e^{\frac{2\pi ix}{n}}$, $\forall x \in G$. In this case, we can see that $K = \{1\}$.
- A is the size m subgroup of H, where $m|(n-1)$. Since K is trivial, KA is automatically a subgroup of H, and $A \cap K = 1$.
- n_c is the number of cosets of A in H, which is $\frac{n-1}{m}$. $\{h_i\}_{i=0}^{n_c}$ are the representatives of these cosets. If x is a cyclic generator for H, then the h_i can be taken to be the powers of x: $h_i = x^i$, $i = 1,...,n_c$.
- $n_o = 2$, because there are only two orbits of G under H. One of these is the trivial orbit, $\{0\}$, and indeed $h \cdot 0 = 0$, $\forall h \in H$. All the nonzero elements $\{1,...,n-1\} \subset G$ are in the same orbit, since any two of these elements differ only by a multiplicative factor in H. Thus we may take our two orbit generators to be $g_1 = 1$ (the generator of the nontrivial orbit) and $g_2 = 0$ (the generator of the tribal orbit).

In light of this last point, we see that these frames trivially satisfy the hypothesis of Corollary 1 since the sets $KAh_i(g_j)$ are simply the cosets Ah_i, which all have the same size as desired. (Note that since we write G additively in this situation, the identity element is 0 instead of 1, so the hypothesis of Corollary 1 effectively becomes that the sets $KAh_i(g_j)$ are the same size for $g_j \neq 0$). Thus the frames from Theorem 2 give us our optimal bound in Theorem 7, and the bound in (52) becomes $\mu \leq \sqrt{n_c}\mu_W$, which is the same bound we saw in Corollary 1. We will explore this connection more in the next section.

VI. Subgroups and Quotients of General Linear Groups

We will now identify a class of groups that yield frames with remarkably low coherence using this framework, a subclass of which consists of the groups used in Theorem 2. Recall that in our original construction of Theorem 2, we chose G to be the additive group $\mathbb{Z}/n\mathbb{Z}$, where n was a prime p, and H was isomorphic to the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$, which contains all the nonzero elements of $\mathbb{Z}/n\mathbb{Z}$ when n is prime. This is equivalent to choosing G and H respectively to be the additive and multiplicative groups of the finite field with p elements, $\mathbb{F}_p$. In this case, H is the simplest example of a general linear group. Indeed, H can be interpreted as the 1-dimensional invertible matrices with entries in $\mathbb{F}_p$. As we will now see, subgroups and quotients of matrix groups over finite fields lend themselves naturally to our construction.

A. Frames from Vector Spaces Over Finite Fields

Recall from our discussion following Theorem 7 that in general our coherence will be closer to the Welch bound if we have fewer orbits, and the sets $KAh_i(g_j)$ are close to each other in size. The optimal case is when their sizes are all equal, in which case we obtain the bound in Corollary 1. Equation (52) in this corollary closely resembles the result from Lemma 2. This is no coincidence, since the condition that the sets $KAh_i(g_j)$ have the same size is equivalent to requiring that each corresponding inner product value arises the same number of times as the inner product between two frame elements. (Recall that we exploited this latter property in deriving Lemma 2.) In a sense, the best case is when we have exactly one nontrivial orbit, so that $n_o = 2$. And if in addition the sets $KAh_i(g_j)$ have the same size for all h_i and $g_j \neq 1$, Corollary 1 shows that the coherence is bounded by a factor of $\sqrt{n_c}$ of the Welch bound.

We saw at the end of Section V that this happens in our original frames constructed in Theorem 2, when G was the additive group of a prime-sized finite field $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ and H the set of automorphisms given by multiplication by elements of $\mathbb{F}_p^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times$. As we remarked at the beginning of this section, H is the simplest example of a general linear group $GL(r, \mathbb{F}_p)$—the multiplicative group of $r \times r$ invertible matrices with entries in $\mathbb{F}_n$ (in this case $r = 1$). It turns out that even higher-dimensional general linear groups fit the framework of Corollary 1. If we set $H := GL(r, \mathbb{F}_p)$ then it is the automorphism group of $G := (\mathbb{F}_p)^r$, the r-dimensional vector space over $\mathbb{F}_p$ (viewed only as an additive abelian group). For any two nonzero vectors $\mathbf{v}_1$ and $\mathbf{v}_2$ in $(\mathbb{F}_p)^r$, there is an invertible matrix $\mathbf{W} \in GL(r, \mathbb{F}_p)$ such that $\mathbf{W}\mathbf{v}_1 = \mathbf{v}_2$, so all nontrivial elements of $(\mathbb{F}_p)^r$ lie in the same orbit under H.

Alternatively, we may view $(\mathbb{F}_p)^r$ as the additive group of the finite field with p^r elements, $\mathbb{F}_{p^r}$, which is a vector space over its subfield $\mathbb{F}_p$. An irreducible representation ρ of $\mathbb{F}_{p^r}$ (and hence of $(\mathbb{F}_p)^r$) is the function

$$\rho(x) = e^{\frac{2\pi i \mathrm{Tr}(x)}{p}}, \tag{54}$$

where $\mathrm{Tr}(x)$ is the *trace* of the field element x, defined as

$$\begin{aligned} \mathrm{Tr} :& \mathbb{F}_{p^r} \to \mathbb{F}_p, \\ \mathrm{Tr}(x) &= x + x^p + x^{p^2} + ... + x^{p^{r-1}}. \end{aligned} \tag{55}$$

The trace function in our context is the sum of the automorphisms of $\mathbb{F}_{p^r}$ fixing the subfield $\mathbb{F}_p$, and is so named because $\mathrm{Tr}(x)$ is the trace of the matrix associated with the linear transformation of multiplication by x. This transformation acts on the additive group of $\mathbb{F}_{p^r}$ viewed as a vector space over $\mathbb{F}_p$. As such, the trace is an additive function: $\mathrm{Tr}(x + y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$, and consequently $\mathrm{Tr}(-x) = -\mathrm{Tr}(x)$. In the case where $r = 1$, the trace becomes the identity function, and we see that as expected we recover a familiar representation of $\mathbb{F}_p$ similar to the ones used in Theorem 2.

We should point out that the *general* form of an irreducible representation of the additive group of $\mathbb{F}_{p^r}$ is $\rho_a(x) := \omega^{\mathrm{Tr}(ax)}$, where $\omega = e^{\frac{2\pi i}{p}}$ and $a \in \mathbb{F}_{p^r}$. This is the image of the function ρ in (54) under the action of k viewed as a matrix in $GL(r, \mathbb{F}_p)$ as just described. As such, it is fitting that the notation "ρ_k" bears resemblance to that of equation (27). Note also that since each of these is a degree-1 representation, each is equal to its own character:

$\chi_k(x) = \rho_k(x)$. Each of the p^r representations ρ_k, $k \in \mathbb{F}_{p^r}$, is unique, and from equation (13) we see that they indeed comprise *all* of the inequivalent irreducible representations of G.

Now, we can concisely describe the group K of character-preserving automorphisms from Theorem 7 as follows: K is simply the set of automorphisms in H which preserve the field trace, $K = \{k \in H \mid \mathrm{Tr}(kx) = \mathrm{Tr}(x),\ \forall x \in G\}$. It can be easily shown that the size of K is $|K| = |H|/|\mathbb{F}_{p^r}^\times| = (p^r - p)\dots(p^r - p^{r-1})$. What is not clear, however, is the form that each element of K will take as a matrix in $H = GL(r, \mathbb{F}_p)$. The same issue arises when we attempt to compute the group A from Theorem 7.

To rectify this issue, we will shift our focus to the interpretation of G as the additive group of the field $\mathbb{F}_{p^r}$. And instead of choosing H to be the entire automorphism group $GL(r, \mathbb{F}_p)$, we will let H be the size-$(p^r - 1)$ subgroup of matrices corresponding to the nonzero field elements $\mathbb{F}_{p^r}^\times$. (Recall, each element of $\mathbb{F}_{p^r}^\times$ acts linearly on $\mathbb{F}_{p^r}$ by multiplication, and as such has a matrix representation when viewed as a linear transformation of $(\mathbb{F}_p)^r$.) In this new setting, the only element of H which fixes the field trace is 1, so K is now the trivial group.

It is reasonable to ask if we lose anything by choosing H to be only a proper subgroup of $GL(r, \mathbb{F}_p)$. But in fact, we can see from Lemma 6 and Theorem 7 that the coherence of our frames depends only on the right cosets of K in H. The following lemma shows that we do not lose anything by choosing H to be $\mathbb{F}_{p^r}^\times$ instead of $GL(r, \mathbb{F}_p)$:

Lemma 7: Let $G = (\mathbb{F}_p)^r$ (which is the additive group of $\mathbb{F}_{p^r}$), and χ a character of G. Let $H_1 = GL(r, \mathbb{F}_p)$ with $K_1 \leq H_1$ the subgroup that fixes χ, and $H_2 = \mathbb{F}_{p^r}^\times \leq H_1$ with corresponding subgroup $K_2 = H_2 \cap K_1$. For every subgroup A_1 of H_1 with $A_1 \cap K_1 = 1$, there is a subgroup A_2 of H_2 with $A_2 \cap K_2 = 1$ such that the groups A_1 and A_2 give rise to the same inner products described by Lemma 6.

Proof: As we touched on above, since our character is a function of the form $\chi(x) = e^{\frac{2\pi i \mathrm{Tr}(ax)}{p}}$, we observe that no nontrivial element of H_2 fixes χ. Thus, $K_2 = 1$. Since the right cosets $K_1\ H_1 = \{K_1 h_1\ :\ h_1 \in H_1\}$ partition H_1, each element $h_2 \in H_2$ must lie in some such coset. We claim that no two elements of H_2 are in the same right coset of K_1. To see this, assume we have h_2 and h_2' in H_2 which lie in the same right coset of K_1. This means that $h_2' h_2^{-1} \in K_1 \cap H_2 = K_2$, hence h_2 and h_2' must be equal. Furthermore, we know that there is one element of H_2 in *each* right coset of K_1 in H_1, since *every* character of G can be written in the form $\chi(h_2(x))$ for some multiplicative field element $h_2 \in H_2$. (This is a well-known fact that can be found, for example, in [27].)

Now, if A_1 is a subgroup of H_1 which intersects K_1 trivially, each element of A_1 must lie in a distinct right coset of K_1. For each element $a_1 \in A_1$, let a_2 be the unique element of H_2 which lies in the same such coset, and let A_2 be the set of all these elements. Clearly A_2 has trivial intersection with K_2, since it is a subset of H_2. The fact that A_2 is itself a group is easy to verify. For example, for elements a_2 and a_2' in A_2, with corresponding elements a_1 and a_1' in A_1, we see that the product $a_2' a_2^{-1}$ is also an element of A_2 since it is the field element lying in the same right coset of K_1 as $a_1' a_1^{-1} \in A_1$. Since elements a in the same right coset of K_1 give rise to the same character $\chi(a(x))$, we see also that the groups A_1 and A_2 will give rise to the same frame inner products as described in Lemma 6. ■

Let us explicitly match this example with the framework of Theorem 7. We note that

- G is the additive group of the vector space $(\mathbb{F}_p)^r$, or equivalently the additive group of the field $\mathbb{F}_{p^r}$.
- $\rho(x) = e^{\frac{2\pi i \mathrm{Tr}(x)}{p}}$.
- $\chi(x) = \rho(x)$, since ρ is a 1-dimensional representation, hence is equal to its own character.
- $H = \mathbb{F}_{p^r}^{\times} = \mathbb{F}_{p^r} \setminus \{0\}$, where G is viewed as the additive group of $\mathbb{F}_{p^r}$. Basic field theory tells us that H is isomorphic to the cyclic group of size $p^r - 1$.
- $K = 1$, since the only field element $h \in H$ such that $\chi(h(x)) = \chi(x)$ is the identity.
- $A = \{a_1, ..., a_m\}$ is any subgroup of H, which will necessarily be a cyclic group of size m, where m is a divisor of $p^r - 1$. Since H is cyclic, there is a unique subgroup for each such m, and it consists of the $\left(\frac{p^r-1}{m}\right)^{th}$ powers in H. Thus, if x is a cyclic generator for H, we may set $y = x^{\frac{p^r-1}{m}}$ and $a_i = y^i$ for each $i = 1, ..., m$.
- $n_c = \frac{p^r-1}{m}$, the number of cosets of A in H. If x is a generator for the cyclic group H, these cosets are $h_i = x^i$, $i = 1, ..., n_c$.
- $n_o = 2$, since again $0 \in \mathbb{F}_{p^r}$ is in its own orbit, and all the nontrivial elements are in their own orbit under H (generated by $1 \in \mathbb{F}_{p^r}$).

Our new frame matrix $\mathbf{M}$ from (33) becomes

$$\mathbf{M} = \begin{bmatrix} \omega^{\mathrm{Tr}(a_1x_1)} & \omega^{\mathrm{Tr}(a_1x_2)} & \dots & \omega^{\mathrm{Tr}(a_1x_n)} & \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \omega^{\mathrm{Tr}(a_mx_1)} & \omega^{\mathrm{Tr}(a_mx_2)} & \dots & \omega^{\mathrm{Tr}(a_mx_n)} & \end{bmatrix}, \tag{56}$$

where we have expressed the elements of our field as $\{x_i\}_{i=1}^n$. If $x_j - x_i = x_\ell$, the inner product between the i^{th} and j^{th} columns now becomes

$$\sum_{a_t} \left(\omega^{\mathrm{Tr}(a_tx_i)}\right)^* \left(\omega^{\mathrm{Tr}(a_tx_j)}\right) = \sum_{a_t} \omega^{\mathrm{Tr}(a_t(x_j - x_i))} \tag{57}$$

$$= \sum_{a_t} \omega^{\mathrm{Tr}(a_tx_\ell)}. \tag{58}$$

We can see from (58) that as in our original frames from Theorem 2, we have exactly $\frac{n-1}{m}$ nontrivial inner product values: one for each element of $\mathbb{F}_{p^r}^\times$ (each of which represents a right coset of K in H). Again, each of these values arises as an inner product the same number of times.

Since these new frames are a generalization our original frames constructed in Theorem 2, it should come as no surprise that the bounds in Theorems 3 and 4 generalizes as well:

Theorem 8: If n is prime power p^r, m a divisor of $n-1$, and $\{a_i\}$ the unique subgroup of $\mathbb{F}_{p^r}^\times$ of size m, then setting $\omega = e^{\frac{2\pi i}{p}}$, and $\kappa := \frac{n-1}{m}$, the coherence μ of our frame $\mathbf{M}$ in (56) satisfies

$$\mu \leq \frac{1}{\kappa}\left((\kappa - 1)\sqrt{\frac{1}{m}\left(\kappa + \frac{1}{m}\right)} + \frac{1}{m}\right). \tag{59}$$

If both p and m are odd, μ satisfies the tighter bound

$$\mu \leq \frac{1}{\kappa}\sqrt{\left(\frac{1}{m} + \left(\frac{\kappa}{2} - 1\right)\beta\right)^2 + \left(\frac{\kappa}{2}\right)^2 \beta^2}, \tag{60}$$

where $\beta = \sqrt{\frac{1}{m}\left(\kappa + \frac{1}{m}\right)}$.

Proof: We present this proof in Appendix A. ■

B. Smaller Alphabets and Frames from Hadamard Matrices

We emphasize that these generalized frames have several advantages over the original frames constructed in Theorem 2. First, the number n of frame vectors is no longer limited to being a prime, but is instead a power of a prime, $n = p^r$. Furthermore, the entries of our frame matrix $\mathbf{M}$ in (56) are no longer n^{th} roots of unity, but rather p^{th} roots of unity. This allows for more practical implementations of our frames. Indeed, while our original frames did achieve low coherence, the entries of the frame vectors came from an alphabet size as large as the frame itself. Thus even for small examples our frames could require an alphabet size of at least several hundred. In our new frames, we could fix p to be a small prime and take a number of frame elements that is substantially larger, yet our frame vectors will only have entries from an alphabet of size p.

For instance, if $p = 2$, then even though our frame can have $n = 2^r$ elements for any r, the matrix $\mathbf{M}$ will always have ± 1 entries. In this case, we have the following:

Theorem 9: When $p = 2$ in our above framework, our frame matrix $\mathbf{M}$ in (56) is a subset of rows of an $n \times n$ Hadamard matrix.

Proof: We already commented above that when $p = 2$, $\mathbf{M}$ will have ± 1 entries. The theorem then follows from the fact that the frame is tight (i.e. the rows of $\mathbf{M}$ are orthogonal with equal norm) by Theorem 6. ■

This is not the first time that frames with ± 1 entries have been explored. For example, [25] designed such frames using codes constructed by [3] and [48], and analyzed the frames' geometry. Figure 2 illustrates the benefit of using our frames to control coherence. Depicting histograms of the inner products resulting from selecting two sets of 341 rows of from a 1024×1024 Hadamard matrix using our method (red) versus randomly (blue), we can see that our construction actually yields just two distinct inner product values in this case, both much closer to zero than the largest magnitude inner products from the random case. In Table I, we compute the coherences of several random vs. group Hadamard frames, and compare to the Welch bound for reference. The group Hadamard frames have consistently lower coherence than the random Hadamard frames, particularly when the frame dimensions m and n are large but the quotient $\kappa = \frac{n-1}{m}$ is small.

C. Difference Sets

On one final note, we point out that in certain cases the group A forms a *difference set* in $\mathbb{F}_{p^r}$, that is, each nonzero element of $\mathbb{F}_{p^r}$ occurs as a difference $a_i - a_j$ the same number of times. In this case, our frames yield examples of those constructed [47] and [15]:

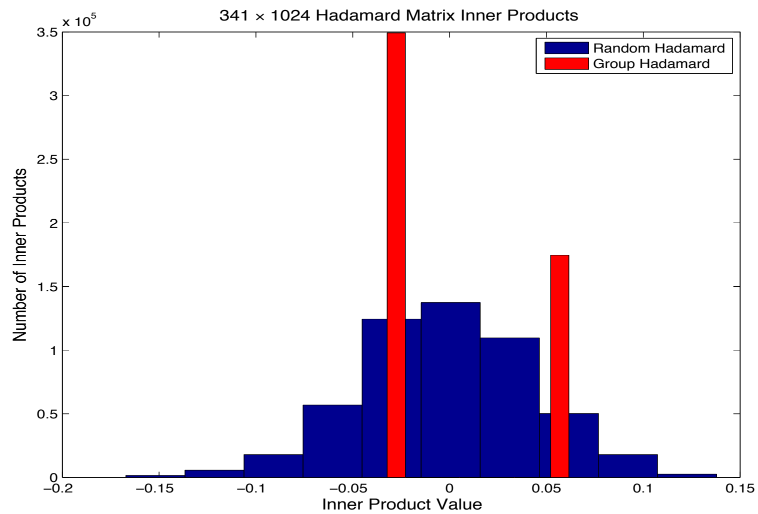


Figure 2: Superimposed histograms of the inner product values between elements of a 341×1024 frame formed from our method of selecting rows of the Hadamard matrix (red) versus selecting the rows randomly (blue). The red values are concentrated to only two points in this case, resulting in coherence closer to zero.

Table I: Coherences for Random vs. Group Hadamards

(n, m)	Random Hadamard	Group Hadamard	$\sqrt{\frac{n-m}{m(n-1)}}$
(256, 51)	.3725	.2549	.1256
(256, 85)	.2941	.1294	.0888
(512, 73)	.3425	.2329	.1085
(1024, 341)	.2023	.0616	.0442
(4096, 455)	.1868	.1253	.0442

Theorem 10: The columns of $\mathbf{M}$ in (56) form a tight equiangular frame if and only if the elements in $A = \{a_i\}_{i=1}^m$ form a difference set in $\mathbb{F}_{p^r}$. In this case, the coherence of $\mathbf{M}$ achieves the Welch bound. In particular, our construction yields a difference set when $\frac{p^r-1}{m} = 2$ and m is odd.

Proof: Again, this follows from the arguments in [47] and [15] (see Theorem 3 of the latter). When $\frac{p^r-1}{m} = 2$, A is the group of squared elements in $\mathbb{F}_{p^r}^{\times}$, which is a well-known difference set when $p^r \equiv 3 \mod 4$ (an example of what is called a "Paley difference set"). [45] This is precisely the case when m is odd. ■

Unfortunately, the Hadamard frames we constructed in the previous section cannot satisfy the condition $\frac{p^r-1}{m} = 2$, since they require that $p = 2$. We can, however, use our construction to produce tight, equiangular frames whose entries are from an alphabet only of size three—the third roots of unity:

Corollary 2: Let $p \equiv 3 \mod 4$ be a prime, r an odd integer, and set $m := \frac{p^r-1}{2}$. Choose the set $A = \{a_i\}_{i=1}^m$ to be the unique subgroup of $\mathbb{F}_{p^r}$ of size m. Then the columns of $\mathbf{M}$ in (56) form a tight equiangular frame whose entries are each one of the distinct p^{th} roots of unity. In particular, when $p = 3$, the entries of $\mathbf{M}$ come from an alphabet of size three.

Proof: Since r is odd, we have $p^r \equiv 3 \mod 4$, so the set A forms a Paley difference set as mentioned in the proof of Theorem 10. Thus the columns of M form a tight, equiangular frame whose elements are integer powers of $\omega = e^{2\pi i/p}$, i.e., the p^{th} roots of unity. ■

In Table II, we list the coherences of several of the tight, equiangular frames arising from Corollary 2, and compare the coherence to when the matrix $\mathbf{M}$ in (56) is formed by randomly choosing the elements $\{a_i\}_{i=1}^m$. As expected, our frames consistently have lower coherence, in this case meeting the Welch bound.

Table II: Coherences for Random vs. Group Matrices with Small Alphabets, $m = \frac{n-1}{2}$

n	Random	Group	$\sqrt{\frac{n-m}{m(n-1)}}$
3^3	.3353	.2035	.2035
3^5	.1577	.0645	.0645
3^7	.0509	.0214	.0214
7^3	.1110	.0542	.0542
11^3	.0674	.0274	.0274

Coherences of $m \times n$ frame matrices formed from rows of the group Fourier matrices for the finite fields $\mathbb{F}_q$, $q = n$. We compare choosing the rows randomly with using the group method from Section VI-A, which produces tight, equiangular frames by Corollary 2. When $n = p^r$, the matrix entries are p^{th} roots of unity.

Table III: Character Table of $SL_2(\mathbb{F}_q)$, q even

Class Representative:	$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$	$\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$	$\begin{bmatrix}c & 0\\ 0 & c^{-1}\end{bmatrix}$	$B\begin{bmatrix}s & 0\\ 0 & s^{-1}\end{bmatrix}B^{-1}$
No. of such classes:	1	1	$\frac{1}{2}(q-2)$	$\frac{1}{2}q$
Size of class:	1	q^2-1	$q(q+1)$	$q(q-1)$
1_G	1	1	1	1
St_G	q	0	1	-1
ρ_χ	$q+1$	1	$\chi(c)+\chi(c^{-1})$	0
π_η	$q-1$	-1	0	$-\eta(s)-\eta(s^{-1})$

Here, $c \in \mathbb{F}_q$ and $s \in \mathbb{F}_{q^2}$, where s is an element of norm 1. B is an invertible matrix with entries in $\mathbb{F}_{q^2}$.

VII. Frames from Special Linear Groups

To show how our framework can be applied to more complicated groups, we will demonstrate how to obtain frames with low coherence in the case where G is the special linear group $SL_2(\mathbb{F}_q)$. Frames of this type were discussed in [39]. This matrix group is easy to describe, but it is nonabelian and has irreducible representations of degree greater than 1, hence will be interesting for our purposes.

Let $\mathbb{F}_q$ be the finite field containing q elements, where q is some integral power of a prime number. Then $SL_2(\mathbb{F}_q)$ is the set of 2×2 determinant-1 matrices with entries in $\mathbb{F}_q$,

$$SL_2(\mathbb{F}_q) := \left\{ \begin{bmatrix} a & b\\ c & d\end{bmatrix} \mid a,b,c,d \in \mathbb{F}_q,\ ad-bc=1 \right\}.$$

It is not difficult to check that the size of this group is $|SL_2(\mathbb{F}_q)| = q(q+1)(q-1)$.

Table III is the character table of $SL_2(\mathbb{F}_q)$ for when q is even (a power of 2). As we can see, in this case the matrices fall into four types of conjugacy classes based on how they diagonalize. The first is simply the identity matrix, $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$. The second consists of the matrices that are not diagonalizable, and have the Jordan canonical form $\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$. These first two conjugacy classes contain all the matrices in $SL_2(\mathbb{F}_q)$ with repeated eigenvalues of 1.

Each conjugacy class of the third type has a representative which is a diagonal matrix: $\begin{bmatrix} c & 0 \\ 0 & c^{-1} \end{bmatrix}$, where $c \in \mathbb{F}_q \setminus \{0, 1\}$. Since the diagonal matrices $\mathrm{diag}(c, c^{-1})$ and $\mathrm{diag}(c^{-1}, c)$ are conjugate to each other, there are $\frac{1}{2}(q-2)$ such classes.

The fourth type of conjugacy class consists of matrices whose eigenvalues do not lie in $\mathbb{F}_q$. These are the matrices that take the form $B \begin{bmatrix} s & 0 \\ 0 & s^{-1} \end{bmatrix} B^{-1}$, where $B \in SL_2(\mathbb{F}_{q^2})$ and $s \in \mathbb{F}_{q^2}$ is one of the *norm-1* elements of $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$, that is, $s^{q+1} = 1$. Note that here $\mathbb{F}_{q^2}$ is the finite field of q^2 elements, which contains $\mathbb{F}_q$ as a subfield. There are $q+1$ elements of $\mathbb{F}_{q^2}$ which satisfy the equation $s^{q+1} = 1$. Of these, the only element lying in $\mathbb{F}_q$ is 1, and the remaining q lie in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. As in the previous case, these q elements pair up to represent a total of $q/2$ distinct conjugacy classes of the fourth type.

There are four types of characters of $SL_2(\mathbb{F}_q)$ for q even, arising as a consequence of the four types of conjugacy classes. The interested reader can refer to [26], [27], [33] to learn in depth how these characters come about, but for now we will give brief descriptions. The first two characters both correspond to degree-1 representations. They include the character of the identity representation 1_G, which maps every element to 1, and that of the Steinberg representation St_G, which maps elements of the various conjugacy classes to the values shown in Table III. For our purposes, the third and fourth types of characters in the last two rows of the table are of greater interest. The third corresponds to what is called an *induced representation*, denoted here as ρ_χ. It is a degree-$(q+1)$ representation built from an underlying nontrivial degree-1 representation χ of the multiplicative group $\mathbb{F}_q^\times$, a cyclic group of size $q-1$. If $\tilde{c}$ is a cyclic generator for $\mathbb{F}_q^\times$ (so that every element can be written as a power of $\tilde{c}$), and we set $\omega_- = e^{\frac{2\pi i}{q-1}}$, then χ is a function of the form $\chi(\tilde{c}^\ell) = \omega_-^{a\ell}$, for some fixed $a \in \{1, 2, ..., q-2\}$. (It is required that a be nonzero modulo $q-1$ in order for ρ_χ to be irreducible.)

The final type of character, denoted π_η, corresponds to a degree-$(q-1)$ *cuspidal representation*. A cuspidal representation is constructed from a degree-1 representation η of the set of norm-1 elements of $\mathbb{F}_{q^2}$, which is a cyclic multiplicative group of size $q+1$. Given a cyclic generator $\tilde{s}$ for this group, and setting $\omega_+ = e^{\frac{2\pi i}{q+1}}$, then η will take the form $\eta(\tilde{s}^\ell) = \omega_+^{h\ell}$, where h is some fixed integer in the set $\{1, 2, ..., q\}$. (Again we require $h \not\equiv 0 \mod q+1$ for irreducibility of π_η.

A. Frames from Induced and Cuspidal Representations

We can now use our previous results to design low-coherence frames in the form of $\mathcal{F}$ in (16) using the characters of $SL_2(\mathbb{F}_q)$ for q even. We emphasize that while explicitly writing out our frame vectors can be cumbersome and requires a certain amount of work in its own right, we will find that *identifying* which representations to use will be quick, as will computing the coherence of the resulting frame.

We will first focus our attention on only the induced representations. For convenience, we will write χ_a and ρ_a respectively for the representations χ and ρ_χ where $\chi(\tilde{c}) = \omega_-^a$. It remains to identify a suitable group A of automorphisms of $SL_2(\mathbb{F}_q)$ under which we can take the image of an induced representation to construct our frames, as prescribed by Theorem 7. In the last section, when our group was just the additive group of a finite field $\mathbb{F}_q$, our automorphisms corresponded to the nonzero field elements which formed the cyclic multiplicative group $\mathbb{F}_q^\times$. These automorphisms were well-described and easy to work with. It turns out that each automorphism φ of $\mathbb{F}_q$ induces an automorphism of $SL_2(\mathbb{F}_q)$ by simply applying φ to the entries of the 2×2 matrices in the special linear group:

$$\varphi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) := \left(\begin{bmatrix} \varphi(a) & \varphi(b) \\ \varphi(c) & \varphi(d) \end{bmatrix}\right). \tag{61}$$

This observation enables us to continue working with the automorphisms of $\mathbb{F}_q$, so we can again choose A to be a subgroup of $\mathbb{F}_q^\times$. If $a' \in A \leq \mathbb{F}_q^\times$, then as an automorphism a' acts on ρ_a as

$$a' \cdot \rho_a = \rho_{a' \cdot a}. \tag{62}$$

Thus, it would be natural to choose for A to act on the representation ρ_1, so that the images under A will be the representations $\{\rho_a \mid a \in A\}$. For the sake of simplicity, we will set $K = 1$ and $H = A$ in our Theorem 7 notation.

One caveat that we now face by choosing this set of automorphisms is the following: notice that each element of A fixes the element $u = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in SL_2(\mathbb{F}_q)$, which means that there is a size-1 orbit $KA(u)$. This means that the bound we gave in Equation (47) of Theorem 7 will be somewhat ineffective. We can get around this problem by noticing that from Equations (50) and (51), the magnitude of the largest inner product will still be small as long as the inner product corresponding to u is small in magnitude. We quickly see this to be the case based on the equation for the inner product given in (34) and the fact that, from Table III, the character values $\rho_a(u)$ are all equal to 1, a relatively small constant. We will give an explicit formula for the inner product corresponding to u in Equation (64), and after normalizing our frame elements (dividing the inner product by the squared norm of a frame element) this inner product becomes very small as q grows.

Since we are working with such a familiar set of automorphisms A, we would like to exploit some of the tools we developed for our frames constructed from finite fields. Consider choosing q such that $q-1$ is some prime p. In this case, χ_a is simply a representation of the cyclic group $\mathbb{Z}/p\mathbb{Z}$, which is isomorphic to the additive group of the field $\mathbb{F}_p$. From the preceding sections, we already have powerful tools at our disposal for bounding certain sums of these characters. Since the character χ_a appears in the main part of the character ρ_a (as shown in Table III), we would like to apply these tools to bound sums of the ρ_a as well. This will allow us to use our bounds from Theorem 8 to obtain even tighter bounds on coherence than those we could obtain from Theorem 7.

Intuitively, if we take m to be a divisor of $p-1$, and let $A = \{a_1, ..., a_m\}$ be the unique size-m subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ (explicitly the set $\{1, ..., p-1\}$ with multiplication modulo p), then we should achieve frames with low coherence by using A to choose the representations ρ_{a_i} to use in our frame matrix $\mathcal{F}$ from (16). Note that from our previous notation,

Now, notice that based on Table III, the characters corresponding to ρ_a and ρ_{-a} are the same (where $-a$ is taken modulo p). This indicates that ρ_a and ρ_{-a} are in fact equivalent representations. If -1 is contained in A and is not equivalent to 1 in $\mathbb{Z}/p\mathbb{Z}$ (which is always the case when q is even, since $p \neq 2$), then for each $a_i \in A$ we also have $-a_i \in A$, and $-a_i \not\equiv a_i$ in $\mathbb{Z}/p\mathbb{Z}$. In this case, the set of chosen representations $\{\rho_a \mid a \in A\}$ has repetition, and using these representations as the rows of $\mathcal{F}$ would yield repeated rows of the Group Fourier Matrix of $SL_2(\mathbb{F}_q)$, and hence would not produce a tight frame (based on Theorem 6). More importantly for our purposes, the resulting frame would not fit our criteria from Theorem 7, which means we could not use the tools we have built to bound its coherence. Therefore, if -1 lies in the unique subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ of size m, we must choose A slightly differently. First, let us explicitly describe how the size-m subgroup decomposes into pairs $\{a, -a\}$:

Lemma 8: Let $q = 2^d$ for some positive integer d, such that $p = q - 1$ is a prime. Take a divisor m of $p-1$, and let A_m be the unique size-m subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$. Then A_m contains -1 if and only if m is even. In this case, $m/2$ is odd, and $A_m = A_{m/2} \cup -A_{m/2}$ where $A_{m/2}$ is the unique size-$\frac{m}{2}$ subgroup and $-A_{m/2} = \{-a \mid a \in A_{m/2}\}$.

Proof: Since p is necessarily odd, -1 generates the unique size-2 subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$, and A_m contains this subgroup if and only if its size m is even.

Since $p = q - 1$ is prime, then writing q in the form 2^d for some integer d, we must have $d > 1$. In this case, m is a divisor of $q - 2 = 2(2^{d-1} - 1)$. In this form, it is clear that $q - 2$ can never be divisible by 4 (since the factor $(2^{d-1} - 1)$ is odd), so neither can its divisor m. Thus, if m is even, $m/2$ must be odd, so $-1 \notin A_{m/2}$. As a result, for any $a \in A_{m/2}$, we must have $-a \in A_m \setminus A_{m/2}$ (since $A_{m/2}$ is a subgroup of A_m). By comparing sizes, we see that A_m must be equal to the union $A_{m/2} \cup -A_{m/2}$. ∎

From Lemma 8, we see that when m is an even divisor of $p-1$, the obvious candidate for the group A is the unique size-$\frac{m}{2}$ subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$, which will ensure that -1 is not in A and that our resulting frame is tight. With this in mind, we will simply assume that we choose m to be odd. The following theorem uses our previous results on frames constructed from finite fields to give a bound on the coherence of the frames we can construct from the induced representations of $SL_2(\mathbb{F}_q)$, for q even.

Theorem 11: Take q a power of 2 such that $q-1$ is a prime p, and let m be an odd divisor of $p - 1$ and $\kappa = \frac{p-1}{2m}$. Let $A = \{a_1, ..., a_m\}$ be the unique subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ of size m, and form $\mathcal{F}$ (as in (16)) from the induced representations ρ_{a_i}. Then the coherence $\mu_\mathcal{F}$ of $\mathcal{F}$ is bounded by

$$\mu_\mathcal{F} \leq \frac{1}{q+1} \max\left(1,\ \frac{1}{\kappa}\left((\kappa - 1)\sqrt{\frac{1}{2m}\left(\kappa + \frac{1}{2m}\right)} + \frac{1}{2m}\right)\right). \tag{63}$$

Proof: From Equation (24) and Table III, we see that the only nontrivial inner products between the columns of $\mathcal{F}$ are those corresponding to the conjugacy classes represented by $u := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in SL_2(\mathbb{F}_q)$ and $w_\ell := \begin{bmatrix} \tilde{c}^\ell & 0 \\ 0 & \tilde{c}^{-\ell} \end{bmatrix} \in SL_2(\mathbb{F}_2)$ for $\ell \in \{1, ..., q-2\}$. These inner products are:

$$u: \quad \sum_{i=1}^{m} d_i \chi_{\rho_{a_i}}(u) = m(q+1) \tag{64}$$

$$\tag{65}$$

$$w_\ell: \quad \sum_{i=1}^{m} d_i \chi_{\rho_{a_i}}(w_\ell) = \sum_{i=1}^{m} (q+1) \cdot (\chi_{a_i}(\tilde{c}^{\ell}) + \chi_{a_i}(\tilde{c}^{-\ell})) \tag{66}$$

$$= (q+1) \sum_{i=1}^{m} (\omega_{-}^{\ell a_i} + \omega_{-}^{-\ell a_i}). \tag{67}$$

From Lemma 8 and the fact that m is odd by assumption, we can see that the union $A \cup -A = \{\pm a_1, ..., \pm a_m\}$ is actually the unique subgroup of $(\mathbb{Z}/p\mathbb{Z})^{\times}$ of size $2m$. If we denote this subgroup as A_{2m}, then we can write the sum in (67) in the form

$$\sum_{i=1}^{m} (\omega_{-}^{\ell a_i} + \omega_{-}^{-\ell a_i}) = \sum_{a \in A_{2m}} \omega_{-}^{\ell a}. \tag{68}$$

But this is just a scaled version of one of our original inner products between the elements of the harmonic frames that we constructed in Theorems 2 and 3, so we can use Theorem 3 to bound its magnitude.

To complete the proof, we simply need to take the maximum of the inner product magnitudes corresponding to the elements u and w_ℓ. This maximum becomes scaled after we normalize the columns of $\mathcal{F}$ by $\sqrt{m(q+1)^2}$, where we obtain the column norm from Equation (25) and the fact that the induced representations are $(q+1)$-dimensional. ■

Table IV: $SL_2(\mathbb{F}_q)$ vs. Gaussian Frame Coherences

Frame Dimensions	$SL_2(\mathbb{F}_q)$	Random Gaussian	Welch Bound
25×60	.2000	.5214	.1540
81×504	.2002	.3482	.1019
243×504	.1111	.2274	.0462

Theorem 11 gives us a recipe for constructing low-coherence frames from the induced representations of $SL_2(\mathbb{F}_q)$ for q even. These frames will consist of $q(q+1)(q-1)$ vectors (one for each element of $SL_2(\mathbb{F}_q)$) which are $m(q+1)^2$-dimensional. Figure 3 shows how our upper bound from the theorem comes decently close to the Welch lower bound on coherence.

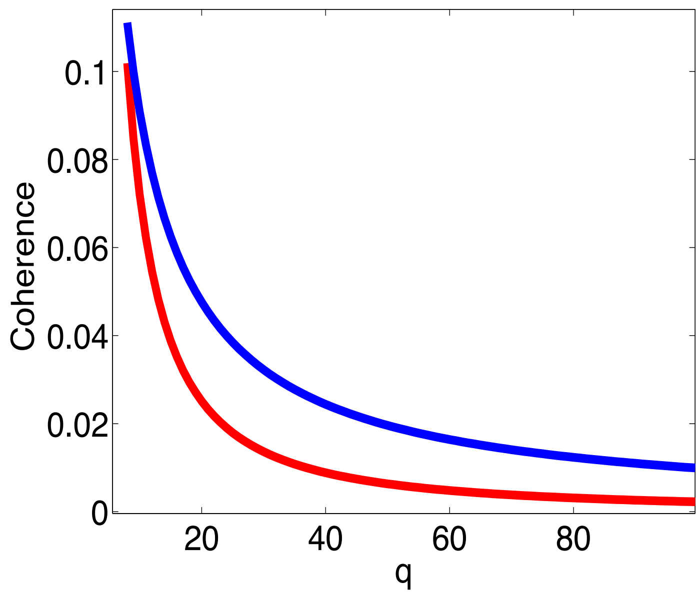


Figure 3: Comparison of the Welch lower bound on coherence with the upper bound given by Theorem 11 for frames constructed from the induced representations of $SL_2(\mathbb{F}_q)$, for q a power of 2 such that $q-1$ is prime. The number of frame vectors is $|SL_2(\mathbb{F}_q)| = q(q+1)(q-1)$, which are $m(q+1)^2$-dimensional. Here, we have fixed $\kappa := \frac{q-2}{2m} = 3$.

In table IV, we provide some explicit values of our frames' coherence, and for comparison we have included the coherence of frames of the same dimensions and number of elements whose coordinates are chosen independently from a Gaussian distribution. While the frame matrix $\mathcal{F}$ can be concretely written out using the explicit forms of the representations given in [26], [27], [33], we will omit this process since we have already described it in depth and since these particular frames tend to have rather large dimensions. We remark that we can obtain similar results using a parallel construction of $\mathcal{F}$ with only cuspidal representations π_η, which works when $q+1$ is prime.

VIII. Satisfying the Coherence Property and the Strong Coherence Property

A closely related quantity to the coherence of a frame $\{f_i\}_{i=1}^n$ in $\mathbb{C}^m$ is the *average coherence* ν, defined as

$$\nu = \frac{1}{n-1} \max_{i\in[n]} \left| \sum_{j\neq i} \langle f_i . f_j \rangle \right| . \tag{69}$$

When discussing the average coherence, the usual quantity μ is sometimes referred to as the *worst-case* coherence. [1] and [25] use the average coherence to describe the following properties of certain frames:

Definition 3: A frame $\{f_i\}_{i=1}^n$ in $\mathbb{C}^m$ with average coherence ν and worst-case coherence μ is said to satisfy the *Coherence Property* if

1) $\mu \leq \frac{0.1}{\sqrt{2\log n}}$, and
2) $\nu \leq \frac{\mu}{\sqrt{m}}$.

It satisfies the *Strong Coherence Property* if

1) $\mu \leq \frac{1}{164 \log n}$, and
2) $\nu \leq \frac{\mu}{\sqrt{m}}$.

These works also give theoretical guarantees on the sparse-signal-recovery abilities of frames satisfying these properties. In particular, they discuss the One-Step Thresholding (OST) algorithm described in [1]. If $F \in \mathbb{C}^{m\times n}$ has columns which form a unit-norm frame, $x \in \mathbb{C}^{n\times 1}$ is a sparse signal, and $e \in \mathbb{C}^{n\times 1}$ is a noise vector, OST produces an estimate $\hat{x}$ for x given $y := Fx + e$. If F satisfies the coherence property, [1] finds regimes in which the support of $\hat{x}$ is equal to that of x with high probability. If F further satisfies the *strong* coherence property, [25] further provides high-probability bounds on the error $||x - \hat{x}||_2$. In the absence of an error vector e, [1] also finds cases where $\hat{x}$ is identically equal to x with high probability.

It turns out that we can explicitly compute the average coherence of our frames from Theorem 7, and indeed any group frame constructed from a set of distinct irreducible representations of the same degree:

Theorem 12: Let G be a finite group of size n and $\rho_1, ..., \rho_m$ a set of distinct nontrivial degree-d irreducible representations of G. Then the columns of the matrix $\mathbf{M} = \sqrt{d}[\text{vec}\rho_i(g_j)] \in \mathbb{C}^{md\times n}$

from (21) form a frame with average coherence $\nu = \frac{1}{n-1}$. If μ is the worst-case coherence of $\mathbf{M}$, then $\nu \leq \frac{\mu}{\sqrt{md}}$ provided that $n \geq 2md$.

Proof: From equations (24) and (25), we have that after normalizing the columns of $\mathbf{M}$, the inner product between the i^{th} and j^{th} columns is

$$\frac{\sum_{t=1}^{m} d \cdot \mathrm{vec}(\rho_t(g_i))^* \mathrm{vec}(\rho_t(g_j))}{md^2} = \frac{1}{md} \sum_{t=1}^{m} \chi_t(g_i^{-1} g_j). \tag{70}$$

Then the average coherence of $\mathbf{M}$ (after normalizing the columns) becomes

$$\nu = \frac{1}{n-1} \max_{i \in [n]} \left| \sum_{j \neq i} \langle f_i, f_j \rangle \right| = \frac{1}{md(n-1)} \max_{i \in [n]} \left| \sum_{j \neq i} \sum_{t=1}^{m} \chi_t(g_i^{-1} g_j) \right| \tag{71}$$

$$= \frac{1}{md(n-1)} \left| \sum_{g \neq 1} \sum_{t=1}^{m} \chi_t(g) \right| \tag{72}$$

$$= \frac{1}{md(n-1)} \left| \sum_{t=1}^{m} \left(\sum_{g \neq 1} \chi_t(g) \right) \right|. \tag{73}$$

Now from basic character theory (see for example [30]), we know that for any character χ_t of a *nontrivial* irreducible representation, we have the relation

$$\frac{1}{|G|} \sum_{g \in G} \chi_t(g) = 0. \tag{74}$$

This is due to the orthogonality of irreducible characters, and the above sum is simply the inner product between χ_t and the trivial character. But this equation gives us

$$\sum_{g \neq 1} \chi_t(g) = -\chi_t(1) = -d, \tag{75}$$

since $\chi_t(1)$ is the degree of the representation ρ_t. Thus,

$$\nu = \frac{1}{md(n-1)} \left| \sum_{t=1}^{m} (-d) \right| = \frac{md}{md(n-1)} = \frac{1}{n-1}. \tag{76}$$

Now from the Welch bound, $\mu \geq \sqrt{\frac{n-md}{md(n-1)}}$. Thus, to show that $\nu \leq \frac{\mu}{\sqrt{md}}$ it is sufficient to show that $\frac{1}{n-1} \leq \frac{1}{\sqrt{md}} \sqrt{\frac{n-md}{md(n-1)}}$, or equivalently that

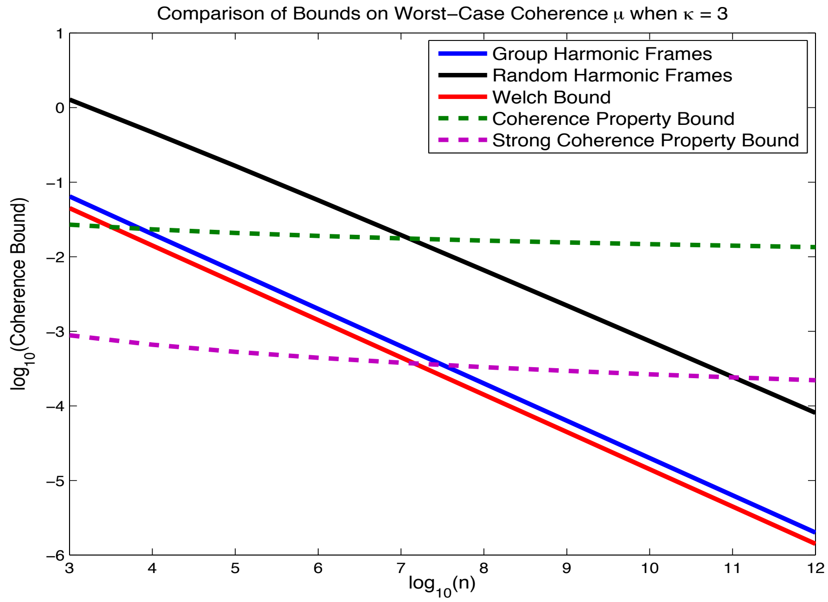
$$md \leq \sqrt{(n-md)(n-1)}. \tag{77}$$

But since $n-1 \geq n-md$, we have $\sqrt{(n-md)(n-1)} \geq n-md$, so (77) is satisfied provided that $2md \leq n$. ■

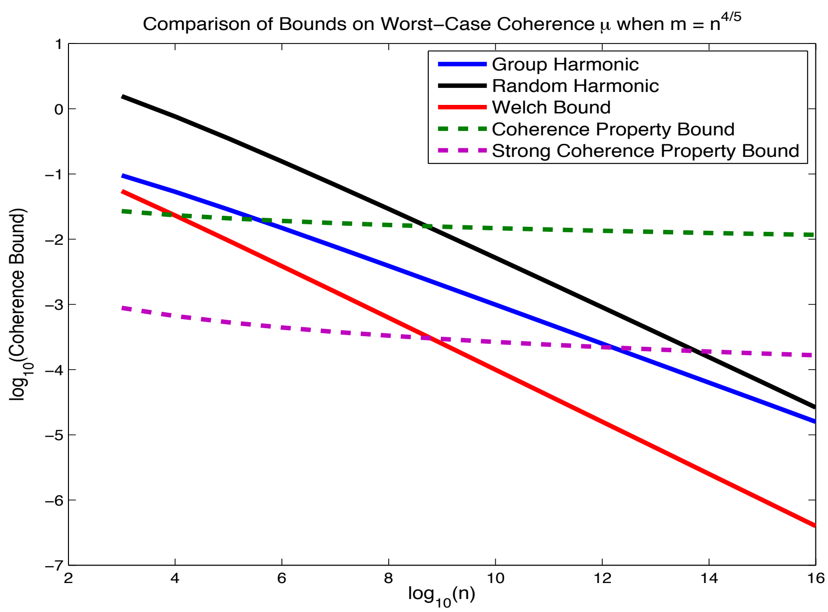
[25] explored the geometry of several types of frames to see when they satisfied the Coherence and Strong Coherence Properties. In particular, they stated the following theorem:

Theorem 13 ([25]): Let F be an $n \times n$ discrete Fourier matrix, $F_{k\ell} = e^{2\pi i k\ell/n}$, $k, \ell = 0, ..., n-1$. Then let M be the submatrix formed by randomly selecting a subset of rows of F, each row independently selected with probability $\frac{m}{n}$, and then normalizing the columns. If $16 \log n \le m \le \frac{n}{3}$, then with probability exceeding $1 - 4n^{-1} - n^{-2}$ the worst-case coherence of M satisfies $\mu_M \le \sqrt{\frac{118(n-m)\log n}{mn}}$.

In Figure 4, we compare this bound with the bound on our harmonic frames from Theorem 3 and the Welch lower bound on coherence, in the regimes where $m = \frac{n-1}{3}$ (i.e. $\kappa = 3$) and when $m = n^{4/5}$. In both cases, we can see that the frames from our group-based construction are guaranteed to satisfy the Coherence and Strong Coherence Properties for a wider range of values of n than random harmonic frames, as suggested by Theorem 13.



(a)



(b)

Figure 4: Comparison of the upper bounds on the coherence of $m \times n$ harmonic frames using our group construction (from Theorem 3) versus choosing rows randomly from a DFT matrix (Theorem 13). In 4(a), $\kappa = \frac{n-1}{m} = 3$, while in 4(b), $m = n^{4/5}$. In both these regimes, the frames from our constructions are guaranteed to satisfy both the Coherence Property and the Strong Coherence Property for smaller dimensions than randomly chosen harmonic frames.

IX. Conclusion

In this paper, we have generalized our methods from [37] to yield a way to select rows of the group Fourier matrix of a finite group G to produce frames with low coherence. By choosing the rows corresponding to the image of a representation under a subgroup of $Aut(G)$, we can reduce the number of distinct inner product values which arise between our frame elements. By exploiting the tightness of the resulting frames, we identified cases in which the coherence comes very close to the Welch lower bound.

We have demonstrated that our method is particularly effective when G is a subgroup or quotient of a group of matrices with entries in a finite field. This is a consequence of the manner in which the field automorphisms permute the elements of G. It is certainly possible that other groups of automorphisms of G can lead to even better coherence when applying our method, though these remain to be explored.

Furthermore, we emphasize that using the character table of G to identify suitable representations to use in our frame allows us to avoid dealing with the explicit forms of the matrices involved in the representations. These matrices are often quite large in dimension and tedious to construct, particularly in the case of the special linear groups we examined in Section VII-A. While exploiting the character table makes coherence calculations relatively painless, however, it is ultimately necessary to use the representation matrices to construct the actual frame vectors. It is desirable to find a class of groups with uncomplicated representations that allow us to build low-coherence frames in a wide variety of dimensions.

Appendix A
Universal Upper Bound On Our Frame Coherence: Proof of Theorems 3, 4, and 8

In this section, we return to the framework of Theorems 3, 4, and 8. Let p be a prime and r a a positive integer, and set our group G (in Theorem 7) to be the finite field $\mathbb{F}_{p^r}$.

Our frame matrix $\mathbf{M}$ from (56) will take the form

$$\mathbf{M} = \begin{bmatrix} \omega^{\mathrm{Tr}(a_1x_1)} & \omega^{\mathrm{Tr}(a_1x_2)} & \dots & \omega^{\mathrm{Tr}(a_1x_n)} & \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \omega^{\mathrm{Tr}(a_mx_1)} & \omega^{\mathrm{Tr}(a_mx_2)} & \dots & \omega^{\mathrm{Tr}(a_mx_n)} & \end{bmatrix}, \tag{78}$$

where $\omega = e^{\frac{2\pi i}{p}}$ and we have expressed the elements of $\mathbb{F}_{p^r}$ as $\{x_i\}_{i=1}^n$. In terms of powers of x, we may relabel these elements as $x_1 = 0$, and $x_i = x^{i-1}$, $i = 2, ..., n = p^r$. Note that with this relabeling, the first column of $\mathbf{M}$ is all 1's.

As we commented before Equation (58), if $x_j - x_i = x_\ell$, the inner product between the i^{th} and j^{th} columns is

$$\sum_{a_t} \left(\omega^{\mathrm{Tr}(a_t x_i)}\right)^* \left(\omega^{\mathrm{Tr}(a_t x_j)}\right) = \sum_{a_t} \omega^{\mathrm{Tr}(a_t(x_j - x_i))} \tag{79}$$

$$= \sum_{a_t} \omega^{\mathrm{Tr}(a_t x_\ell)}. \tag{80}$$

We will be making extensive use of the sums in (80) in this section, so we will make the following definition:

Definition 4: For any $z \in \mathbb{F}_{p^r}$ and A a subgroup of $\mathbb{F}_{p^r}^\times$, we will define c_z to be the normalized inner product sum corresponding to z, that is,

$$c_z = \frac{1}{m} \sum_{a \in A} \omega^{\mathrm{Tr}(az)}, \tag{81}$$

where $\omega = e^{2\pi i/p}$.

The following property of the values c_z is simple, but worth establishing:

Lemma 9: For any $z \in \mathbb{F}_{p^r}$, we have $c_z^* = c_{-z}$.

Proof: Expanding c_z as a sum, we have

$$(c_z)^* = \left(\frac{1}{m} \sum_{a \in A} \omega^{\mathrm{Tr}(za)}\right)^* \tag{82}$$

$$= \frac{1}{m} \sum_{a \in A} \omega^{-\mathrm{Tr}(za)} \tag{83}$$

$$= c_{-z}. \tag{84}$$

■

Recall that the set of nonzero field elements $\mathbb{F}_{p^r}^\times$ is a cyclic group under multiplication, so let x be a multiplicative generator. The elements of $\mathbb{F}_{p^r}$ can now be expressed as $\{0, 1, x, ..., x^{p^r-1}\}$. The inner product corresponding to 0 is simply $c_0 = 1$, which arises only when taking the inner product of a frame element with itself. The nontrivial inner products are thus c_{x^i}, for $i = 0, ..., p^r - 1$.

We point out that if A is a size-m multiplicative subgroup, it is unique (since $\mathbb{F}_{p^r}$ is cyclic) and is a cyclic group generated by x^κ, where $\kappa = \frac{p^r-1}{m}$. The cosets of A are $A, xA, ..., x^{\kappa-1}A$. One interesting observation is that elements in the same coset of A give rise to the same inner product value:

Lemma 10: If z is in the coset x^iA, then $c_z = c_{x^i}$.

Proof: Write $z = x^i a_z$, for some $a_z \in A$. Then,

$$c_z = \sum_{a \in A} \omega^{\mathrm{Tr}(x^i a_z \cdot a)} \tag{85}$$

$$= \sum_{a \in A} \omega^{\mathrm{Tr}(x^i a)}, \tag{86}$$

where $\omega = e^{2\pi i/p}$ and the last equality follows from the fact that since A is a group, multiplication by a_z simply permutes its elements. ■

In light of Lemma 10, we see concretely that there is indeed only a single nontrivial inner product value for each coset of A, and each arises with the same multiplicity (because each coset has the same number of elements). Furthermore, since $\{1, x, ..., x^{\kappa-1}\}$ is a set of representatives for each of the cosets of A, we only need to be concerned with the values c_{x^i}, $i = 0, 1, ..., \kappa - 1$. The largest absolute value of these will be the coherence.

Lemma 11: The values $c_1, c_x, ..., c_{x^{\kappa-1}}$ satisfy the equation

$$1 + mc_1 + mc_x + ... + mc_{x^{\kappa-1}} = 0, \tag{87}$$

where m is the size of A.

Proof: If we expand the sum in (87) using the fact that each of the m elements $z \in x^dA$ satisfies $c_z = c_{x^d}$, and that $c_0 = 1$, we get

$$1 + \sum_{d=1}^{\kappa-1} mc_{x^d} = \sum_{z \in \mathbb{F}_{p^r}} c_z \tag{88}$$

$$= \sum_{a \in A} \sum_{z \in \mathbb{F}_{p^r}} \omega^{\mathrm{Tr}(za)}, \tag{89}$$

where $\omega = e^{\frac{2\pi i}{p}}$. But the function $\chi_{reg}(y) := \sum_{z \in \mathbb{F}_{p^r}} \omega^{\mathrm{Tr}(zy)}$ which arises as the internal sum in (89) is the well-known character of the "regular representation" of $\mathbb{F}_{p^r}$, which is equal to p^r if $y = 0$ and 0 otherwise [30]. Since no elements of A are 0, we see that (89) sums to zero.

■

Our following work will involve taking many sums and products of field elements, and determining in which coset of A they lie. While it is in general easy to determine in which coset a product lies (for example, if $z_1 \in x^{i_1}A$ and $z_2 \in x^{i_2}A$, then $z_1 z_2 \in x^{i_1+i_2}A$), it is often not obvious in which coset a sum lies. To get around this problem, we will make use of the following quantities:

Definition 5: Given two cosets x_1A and x_2A, we define the *translation degree* from x_1A to x_2A to be the quantity

$$N_{x_1A,x_2A} = \#\{z \in x_1A \mid 1+z \in x_2A\} = |1 + x_1A \cap x_2A|. \tag{90}$$

Likewise, we define $N_{x_1A,0}$ and N_{0,x_2A} (the translation degrees from x_1A to 0 and from 0 to x_2A, respectively) to be

$$N_{x_1A,0} = |\{-1\} \cap x_1A|, \tag{91}$$

$$N_{0,x_2A} = |\{1\} \cap x_2A|. \tag{92}$$

We will quickly point out a simple property of the translation degrees:

Lemma 12: Set $H = \mathbb{F}_{p^r}^{\times}$. For any coset x_0A, we have

$$N_{x_0K,0} + \sum_{x_iK \in H/A} N_{x_0A,x_iA} = |x_0A|.$$

In particular, if $-1 \in x_0A$, this equation reduces to

$$1 + N_{x_0A,A} + N_{x_0A,xA} + N_{x_0A,x^2A} + ... + N_{x_0A,x^{\kappa-1}A} = m,$$

and if $-1 \notin x_0A$, this equation becomes

$$N_{x_0A,A} + N_{x_0A,xA} + N_{x_0A,x^2A} + ... + N_{x_0A,x^{\kappa-1}A} = m.$$

Proof: This simply follows from the observation that any of the m elements of x_0A, when added to 1, must either be equal to 0 or lie in exactly one of the cosets $x_iA \in H/A$.

∎

The following lemma will be instrumental in bounding these inner product values.

Lemma 13: Let $\mathbf{c} = [c_1, c_x, c_{x^2}, ..., c_{x^{\kappa-1}}]^T$, and let F be the scaled $\kappa \times \kappa$ Fourier matrix with entries defined by $F_{ij} = \gamma^{(i-1)(j-1)}$, where $\gamma = e^{2\pi i/\kappa}$. Then, if we let $\mathbf{w} := [w_1, ..., w_\kappa]^T = F\mathbf{c}$ so that $w_{d+1} = \sum_{t=0}^{\kappa-1} \gamma^{td} c_{x^t}$ for $d = 0, 1, ..., \kappa - 1$, we have

$$w_1 = -\frac{1}{m}, \tag{93}$$

$$|w_i| = \sqrt{\frac{1}{m}\left(\kappa + \frac{1}{m}\right)}, \qquad i \neq 1. \tag{94}$$

Proof: For any $d = 0, 1, ..., \kappa - 1$, we have

$$|w_{d+1}|^2 = \left(\sum_{t=0}^{\kappa-1} \gamma^{td} c_{x^t}\right)\left(\sum_{\ell=0}^{\kappa-1} \gamma^{\ell d} c_{x^\ell}\right)^* \tag{95}$$

$$= \left(\sum_{t=0}^{\kappa-1} \gamma^{td} c_{x^t}\right)\left(\sum_{\ell=0}^{\kappa-1} \gamma^{-\ell d} c_{-x^\ell}\right) \tag{96}$$

$$= \sum_{t=0}^{\kappa-1}\sum_{\ell=0}^{\kappa-1} \gamma^{(t-\ell)d} c_{x^t} c_{-x^\ell} \tag{97}$$

$$= \sum_{s=0}^{\kappa-1}\sum_{\ell=0}^{\kappa-1} \gamma^{sd} c_{x^{s+\ell}} c_{-x^\ell} \tag{98}$$

$$= \sum_{s=0}^{\kappa-1} \gamma^{sd} \sum_{\ell=0}^{\kappa-1} c_{x^{s+\ell}} c_{-x^\ell} \tag{99}$$

Now, we note that

$$
\begin{aligned}
m^2 c_{x^{s+\ell}} c_{-x^\ell} &= \left(\sum_{a\in A} \omega^{\mathrm{Tr}(x^{s+\ell}a)}\right)\left(\sum_{a'\in A} \omega^{\mathrm{Tr}(-x^\ell a')}\right) && (100)\\
&= \sum_{a,a'\in A} \omega^{\mathrm{Tr}(x^{s+\ell}a - x^\ell a')} && (101)\\
&= \sum_{a,a'\in A} \omega^{\mathrm{Tr}(-x^\ell a'(1-x^s a a'^{-1}))} && (102)\\
&= \sum_{a',a''\in A} \omega^{\mathrm{Tr}(-x^\ell a'(1-x^s a''))} && (103)\\
&= \sum_{t=0}^{\kappa-1} \sum_{\substack{\{a',a''\in A\ :\\ 1-x^s a''\in x^t A\}}} \omega^{\mathrm{Tr}(-x^\ell a'(1-x^s a''))} && (104)\\
&\qquad + \sum_{\substack{\{a',a''\in A\ :\\ 1-x^s a''=0\}}} 1 \\
&= \sum_{t=0}^{\kappa-1} N_{-x^s A, x^t A}\left(\sum_{a'''\in A} \omega^{\mathrm{Tr}(-x^t x^\ell a''')}\right) && (105)\\
&\qquad + \sum_{a'\in A} N_{-x^s A,0} && (106)\\
&= m\sum_{t=0}^{\kappa-1} N_{-x^s A, x^t A}\cdot c_{-x^{t+\ell}} + mN_{-x^s A,0} && (107)
\end{aligned}
$$

Now we can substitute this into (99), and we obtain:

$$
\begin{aligned}
|w_{d+1}|^2 &= \sum_{s=0}^{\kappa-1} \gamma^{sd} \sum_{\ell=0}^{\kappa-1}\left(\frac{1}{m}\left(\sum_{t=0}^{\kappa-1} N_{-x^s A, x^t A}\cdot c_{-x^{t+\ell}} + N_{-x^s A,0}\right)\right) && (108)\\
&= \sum_{s=0}^{\kappa-1} \gamma^{sd} \frac{1}{m}\left(\sum_{t=0}^{\kappa-1} N_{-x^s A, x^t A}\sum_{\ell=0}^{\kappa-1} c_{-x^{t+\ell}} + \sum_{\ell=0}^{\kappa-1} N_{-x^s A,0}\right) && (109)\\
&= \sum_{s=0}^{\kappa-1} \gamma^{sd} \frac{1}{m}\left(\sum_{t=0}^{\kappa-1} N_{-x^s A, x^t A}\left(-\frac{1}{m}\right) + \kappa N_{-x^s A,0}\right) && (110)\\
&= -\frac{1}{m^2}\sum_{s=0}^{\kappa-1} \gamma^{sd} \sum_{t=0}^{\kappa-1} N_{-x^s A, x^t A} + \frac{1}{m}\sum_{s=0}^{\kappa-1} \gamma^{sd}\kappa N_{-x^s A,0} && (111)\\
&= -\frac{1}{m^2}\sum_{s=0}^{\kappa-1} \gamma^{sd}\left(m - N_{-x^s A,0}\right) + \frac{\kappa}{m}\sum_{s=0}^{\kappa-1} \gamma^{sd} N_{-x^s A,0} && (112)
\end{aligned}
$$

where (110) follows from Equation (87), and (112) follows from Lemma 12. Note that $N_{-x^sA,0}$ is equal to 1 if $s=0$ and equal to 0 otherwise. Thus, (112) becomes

$$|w_{d+1}|^2 = -\frac{1}{m^2}\left((m-1) + m\sum_{s=1}^{\kappa-1}\gamma^{sd}\right) + \frac{\kappa}{m}. \tag{113}$$

Now, if $d \neq 0$, then $\sum_{s=1}^{\kappa-1}\gamma^{sd} = -1$, and after rearranging terms we obtain

$$|w_{d+1}|^2 = \frac{1}{m}\left(\kappa + \frac{1}{m}\right). \tag{114}$$

If $d=0$, then $\sum_{s=1}^{\kappa-1}\gamma^{sd} = m$, and (113) gives us $|w_1|^2 = \frac{1}{m^2}$. In fact, in this case, we can compute w_1 explicitly, since

$$w_1 = \sum_{t=0}^{\kappa-1} c_{x^t} = -\frac{1}{m}. \tag{115}$$

■

We can now use Lemma 13 to bound the coherence of our frames constructed from finite fields.

Theorem 14: Let $G = \mathbb{F}_{p^r}$ be the finite field with elements $\{x_1, ..., x_{p^r}\}$, and $H = \mathbb{F}_{p^r}^{\times}$ the (cyclic) multiplicative group of the nonzero field elements. If A is the unique subgroup of H of size m, with elements $\{a_1, ..., a_m\}$, and $\mathbf{M}$ is the frame with columns defined in (78), then the coherence μ of $\mathbf{M}$ is upper-bounded by

$$\mu \leq \frac{1}{\kappa}\left((\kappa-1)\sqrt{\frac{1}{m}\left(\kappa+\frac{1}{m}\right)} + \frac{1}{m}\right). \tag{116}$$

Proof: The proof follows from Lemma 13. Using the notation of this lemma, we may write $\mathbf{c} = \frac{1}{\kappa}F^*\mathbf{w}$, so that

$$|c_{x^d}| = \frac{1}{\kappa}\left|\sum_{j=1}^{\kappa}\gamma^{d(j-1)}w_j\right| \tag{117}$$

$$\leq \frac{1}{\kappa}\sum_{j=1}^{\kappa}|w_j| \tag{118}$$

$$= \frac{1}{\kappa}\left((\kappa-1)\sqrt{\frac{1}{m}\left(\kappa+\frac{1}{m}\right)} + \frac{1}{m}\right), \tag{119}$$

where (118) follows from the triangle inequality and (119) follows from Lemma 13. Since the coherence is equal to the largest value among the $|c_{x^d}|$, $d = 0, ..., p^r - 1$, the result now follows immediately. ■

Recall from Theorems 4 and 8 that when the size m of A happens to be an odd integer, we can derive even tighter bounds on coherence, provided that p is an odd prime. (Note that in our original framework of Theorem 2, when m was taken to be a divisor of $p-1$, the only case where p could be even was when $p = 2$ and $m = 1$ in which case our frames would be 1-dimensional and trivially have coherence equal to 1.) We will prove this result shortly, but we first present the following equivalent condition on A for when its size is even or odd.

Lemma 14: Let p be a prime, r an integer, m a divisor of $p^r - 1$, and $\kappa := \frac{p^r-1}{m}$. Let $\mathbb{F}_{p^r}$ be the finite field with p^r elements, whose multiplicative group $\mathbb{F}_{p^r}^\times$ has cyclic generator x, and let A be the unique subgroup of $\mathbb{F}_{p^r}^\times$ of size m. Then $-1 \in A$ if and only if either p or m is even. If p and m are both odd, then κ is even and $-1 \in x^{\frac{\kappa}{2}} A$.

Proof: If p is even, that is $p = 2$, then $-1 \equiv 1$ in $\mathbb{F}_{p^r}$, so trivially $-1 \in A$. If p is odd, then the order m of A is even if and only if A has a subgroup of size 2, which means there is a nontrivial element in A which is a root of the polynomial $X^2 - 1$. The element -1 is the only such root.

If both m and p are odd, then $p^r - 1$ must be even, hence so is $\kappa = \frac{p^r-1}{m}$. In this case, since the square of -1 obviously lies in A (which is equal to $x^\kappa A$), we must have $-1 \in x^{\frac{\kappa}{2}} A$. ■

We need one more tool before we can prove our tighter bound:

Lemma 15: Let p, r, m, κ, x and A be defined as in Lemma 14 and $\mathbf{w} = [w_1, ..., w_\kappa]^T$ be defined as in Lemma 13. If either p or m is even ($-1 \in A$) then for any $d = 0, 1, ..., \kappa - 1$, we have $c_{x^d} = c^*_{x^d}$, and for any $i = 2, 3, ..., \kappa$ we have $w^*_i = w_{\kappa-i+2}$. If p and m are both odd ($-1 \in x^{\frac{\kappa}{2}} A$), then $c_{x^d} = c^*_{x^{d+\kappa/2}}$ and $w^*_i = (-1)^{i-1} w_{\kappa-i+2}$.

Proof: As usual, set $\omega = e^{2\pi i/p}$ and $\gamma := e^{2\pi i/\kappa}$. If $-1 \in A$, then multiplication by -1

permutes the elements of A, so we have

$$c_{x^d}^* = \left(\frac{1}{m}\sum_{a\in A}\omega^{x^d a}\right)^* \tag{120}$$

$$= \frac{1}{m}\sum_{a\in A}\omega^{-x^d a} \tag{121}$$

$$= \frac{1}{m}\sum_{a\in A}\omega^{x^d a} \tag{122}$$

$$= c_{x^d}. \tag{123}$$

It follows that c_{x^d} is real. Furthermore, in this case we have

$$w_i^* = \left(\sum_{j=1}^{\kappa}\gamma^{(i-1)(j-1)}c_{x^{j-1}}\right)^* \tag{124}$$

$$= \sum_{j=1}^{\kappa}\gamma^{-(i-1)(j-1)}c_{x^{j-1}}^* \tag{125}$$

$$= \sum_{j=1}^{\kappa}\gamma^{(-i+1)(j-1)}c_{x^{j-1}} \tag{126}$$

$$= \sum_{j=1}^{\kappa}\gamma^{(\kappa-i+1)(j-1)}c_{x^{j-1}} \tag{127}$$

$$= \sum_{j=1}^{\kappa}\gamma^{((\kappa-i+2)-1)(j-1)}c_{x^{j-1}} \tag{128}$$

$$= w_{\kappa-i+2}. \tag{129}$$

Now, if instead $-1 \in x^{\frac{\kappa}{2}}A$, then multiplication by $-x^{\frac{\kappa}{2}}$ permutes the elements of A, and we have

$$c_{x^d} = \frac{1}{m}\sum_{a\in A}\omega^{x^d a} \tag{130}$$

$$= \frac{1}{m}\sum_{a\in A}\omega^{-x^d x^{\frac{\kappa}{2}} a} \tag{131}$$

$$= \left(\frac{1}{m}\sum_{a\in A}\omega^{x^{d+\frac{\kappa}{2}} a}\right)^* \tag{132}$$

$$= c_{x^{d+\kappa/2}}^*. \tag{133}$$

Also in this case, we may write

$$w_i^* = \left(\sum_{j=1}^{\kappa} \gamma^{(i-1)(j-1)} c_{x^{j-1}}\right)^* \tag{134}$$

$$= \sum_{j=1}^{\kappa} \gamma^{-(i-1)(j-1)} c^*_{x^{j-1}} \tag{135}$$

$$= \sum_{j=1}^{\kappa} \gamma^{-(i-1)(j-1)} c_{x^{j-1+\frac{\kappa}{2}}} \tag{136}$$

$$= \sum_{j=1}^{\kappa} \gamma^{-(i-1)(j-1+\frac{\kappa}{2})} \gamma^{(i-1)\frac{\kappa}{2}} c_{x^{j-1+\frac{\kappa}{2}}} \tag{137}$$

$$= \gamma^{(i-1)\frac{\kappa}{2}} \sum_{j=1}^{\kappa} \gamma^{(\kappa-i+1)(j-1+\frac{\kappa}{2})} c_{x^{j-1+\frac{\kappa}{2}}} \tag{138}$$

$$= \gamma^{(i-1)\frac{\kappa}{2}} w_{\kappa-i+2} \tag{139}$$

$$= (-1)^{i-1} w_{\kappa-i+2}, \tag{140}$$

where the last line follows from the fact that $\gamma^{\frac{\kappa}{2}} = -1$. This completes the proof of the lemma. ■

We are now equipped to prove the second part of Theorem 8, which we restate here for convenience:

Theorem 15: Let p be a prime, r a positive integer, m a divisor of $p^r - 1$, and $A = \{a_i\}_{i=1}^m$ the unique subgroup of $\mathbb{F}_{p^r}^{\times}$ of size m. Then setting $\omega = e^{\frac{2\pi i}{p}}$ and $\kappa := \frac{p^r-1}{m}$, if both p and m are odd, the coherence μ of our frame $\mathbf{M}$ in (78) satisfies

$$\mu \leq \frac{1}{\kappa}\sqrt{\left(\frac{1}{m} + \left(\frac{\kappa}{2} - 1\right)\beta\right)^2 + \left(\frac{\kappa}{2}\right)^2 \beta^2}, \tag{141}$$

where $\beta = \sqrt{\frac{1}{m}\left(\kappa + \frac{1}{m}\right)}$.

Proof: Since both p and m are odd, then from Lemma 14 we know that κ is even and -1 lies in the coset $x^{\frac{\kappa}{2}}A$. There is a 1-1 correspondence between the set of integers $\{1, ..., \kappa\}$ and itself which sends $j \mapsto \kappa - j + 2 \mod \kappa$, for $j = 1, ..., \kappa$. This mapping fixes the singletons $\{1\}$ and $\{\frac{\kappa}{2} + 1\}$ and interchanges the elements in the pairs $\{j, \kappa - j + 2\}$ for $j = 2, ..., \frac{\kappa}{2}$.

As in Lemma 13, set $\mathbf{c} = [c_1, c_x, c_{x^2}, ..., c_{x^{\kappa-1}}]^T$ and $\mathbf{w} := [w_1, ..., w_\kappa]^T = F\mathbf{c}$, where F is the scaled $\kappa \times \kappa$ Fourier matrix with entries $F_{ij} = \gamma^{(i-1)(j-1)}$, where $\gamma = e^{2\pi i/\kappa}$. Since $-1 \in x^{\frac{\kappa}{2}A}$, then by Lemmas 13 and 15 we have

$$w_j \cdot w_{\kappa-j+2} = w_j \left(\left((-1)^{j-1} \right)^{-1} w_j^* \right) \tag{142}$$

$$= (-1)^{j-1} |w_j|^2 \tag{143}$$

$$= (-1)^{j-1} \beta^2 \tag{144}$$

where $\beta = \sqrt{\frac{1}{m}\left(\kappa + \frac{1}{m}\right)}$.

We quickly note that given integers i and j, the conjugate of $\gamma^{-(i-1)(j-1)}$ can be expressed as

$$\left(\gamma^{-(i-1)(j-1)}\right)^* = \gamma^{-(i-1)(-j+1)} \tag{145}$$

$$= \gamma^{-(i-1)(\kappa-j+1)} \tag{146}$$

$$= \gamma^{-(i-1)((\kappa-j+2)-1)}. \tag{147}$$

Note that the inverse of F is $\frac{1}{\kappa}F^*$. From the equation $\mathbf{c} = \frac{1}{\kappa}F^*\mathbf{w}$, we may write

$$c_{x^{i-1}} = \frac{1}{\kappa} \sum_{j=1}^{\kappa} \gamma^{-(i-1)(j-1)} w_j. \tag{148}$$

Now we can group the terms of the summation of $c_{x^{i-1}}$ by our above subsets of indices ($\{j, \kappa - j + 2\}$ for $j = 2, \ldots, \frac{\kappa}{2}$) as follows:

$$c_{x^{i-1}} = \frac{1}{\kappa} \left[w_1 + \gamma^{-(i-1)\frac{\kappa}{2}} w_{\frac{\kappa}{2}+1} + \sum_{j=2}^{\frac{\kappa}{2}} \left(\gamma^{-(i-1)(j-1)} w_j + \gamma^{-(i-1)((\kappa-j+2)-1)} w_{\kappa-j+2} \right) \right]. \tag{149}$$

We know from Lemma 13 that $w_1 = -\frac{1}{m}$ and $|w_{\frac{\kappa}{2}+1}| = \beta$. Also,

$$\gamma^{-(i-1)\frac{\kappa}{2}} = (\gamma^{\frac{\kappa}{2}})^{-(i-1)} = (-1)^{-(i-1)} = (-1)^{i-1},$$

and from Lemma 15 we know that $w_{\frac{\kappa}{2}+1} = (-1)^{\frac{\kappa}{2}} w^*_{\frac{\kappa}{2}+1}$. Thus, if $\frac{\kappa}{2}$ is even we have that $w_{\frac{\kappa}{2}+1}$ is purely real, so $\gamma^{-(i-1)\frac{\kappa}{2}} w_{\frac{\kappa}{2}+1} = \pm\beta$. And if $\frac{\kappa}{2}$ is odd, we have that $w_{\frac{\kappa}{2}+1}$ is purely imaginary, in which case $\gamma^{-(i-1)\frac{\kappa}{2}} w_{\frac{\kappa}{2}+1} = \pm i\beta$.

From these observations and Lemma 15, we have

$$\gamma^{-(i-1)(j-1)} w_j + \gamma^{-(i-1)((\kappa-j+2)-1)} w_{\kappa-j+2}$$

$$= \gamma^{-(i-1)(j-1)} w_j + (-1)^{j-1} \gamma^{-(i-1)((\kappa-j+2)-1)} w_j^* \tag{150}$$

$$= \gamma^{-(i-1)(j-1)} w_j + (-1)^{j-1} \left(\gamma^{-(i-1)(j-1)} w_j \right)^*. \tag{151}$$

If j is even (151) becomes $2i\Im(\gamma^{-(i-1)(j-1)}w_j)$ and if j is odd it becomes $2\Re(\gamma^{-(i-1)(j-1)}w_j)$, where $\Im(z)$ and $\Re(z)$ denote the imaginary and real parts of the complex number z respectively. If we define the phase θ_j such that $w_j = \beta e^{i\theta_j}$, we can further express these as

$$2i\Im(\gamma^{-(i-1)(j-1)}w_j) = 2i\beta \sin\left(\theta_j - \frac{2\pi}{\kappa}(i-1)(j-1)\right) \tag{152}$$

and

$$2\Re(\gamma^{-(i-1)(j-1)}w_j) = 2\beta \cos\left(\theta_j - \frac{2\pi}{\kappa}(i-1)(j-1)\right). \tag{153}$$

To simplify our notation, we will define

$$\tilde{\theta}_j := \theta_j - \frac{2\pi}{\kappa}(i-1)(j-1),$$

allowing us to write the summation in (149) as

$$\sum_{j=2}^{\frac{\kappa}{2}} \left(\gamma^{-(i-1)(j-1)}w_j + \gamma^{-(i-1)((\kappa-j+2)-1)}w_{\kappa-j+2}\right)$$
$$= \sum_{j \text{ even}} 2i\beta \sin(\tilde{\theta}_j) + \sum_{j \text{ odd}} 2\beta \cos(\tilde{\theta}_j).$$

Now, we can bound the coherence by

$$\mu \le \max_{\{\theta_j\}} \max_i |c_{x^{i-1}}| \le \max_i \max_{\{\theta_j\}} |c_{x^{i-1}}|,$$

and from our above discussion this becomes

$$\max_{\{\tilde{\theta}_j\}} \frac{1}{\kappa}\left| -\frac{1}{m} \pm \beta + \sum_{j \text{ even}} 2i\beta \sin(\tilde{\theta}_j) + \sum_{j \text{ odd}} 2\beta \cos(\tilde{\theta}_j)\right| \tag{154}$$

if $\frac{\kappa}{2}$ is even, and

$$\max_{\{\tilde{\theta}_j\}} \frac{1}{\kappa}\left| -\frac{1}{m} \pm i\beta + \sum_{j \text{ even}} 2i\beta \sin(\tilde{\theta}_j) + \sum_{j \text{ odd}} 2\beta \cos(\tilde{\theta}_j)\right| \tag{155}$$

if $\frac{\kappa}{2}$ is odd.

If we set

$$n_e := \#\{j \text{ even} \mid 2 \le j \le \frac{\kappa}{2}\}$$

and

$$n_o := \#\{j \text{ odd} \mid 2 \le j \le \frac{\kappa}{2}\},$$

then by speculation, (154) becomes bounded by

$$\frac{1}{\kappa}\left|\frac{1}{m}+\beta+n_e 2i\beta+n_o 2\beta\right|=\frac{1}{\kappa}\sqrt{\left(\frac{1}{m}+\beta(1+2n_o)\right)^2+(2n_e\beta)^2} \tag{156}$$

and (155) becomes bounded by

$$\frac{1}{\kappa}\left|\frac{1}{m}+i\beta+n_e 2i\beta+n_o 2\beta\right|=\frac{1}{\kappa}\sqrt{\left(\frac{1}{m}+2n_o\beta\right)^2+\beta^2(1+2n_e)^2} \tag{157}$$

Finally, we note that when $\frac{\kappa}{2}$ is even, then $n_e=\frac{\kappa}{4}$ (half the numbers between 1 and $\frac{\kappa}{2}$, inclusive, are even), and hence $n_o=\left(\frac{r}{\kappa}-1\right)-n_e=\frac{\kappa}{4}-1$. Thus, (156) becomes

$$\frac{1}{\kappa}\sqrt{\left(\frac{1}{m}+\beta\left(1+2\left(\frac{\kappa}{4}-1\right)\right)\right)^2+\left(2\cdot\frac{\kappa}{4}\cdot\beta\right)^2} \tag{158}$$

$$=\frac{1}{\kappa}\sqrt{\left(\frac{1}{m}+\left(\frac{\kappa}{2}-1\right)\beta\right)^2+\left(\frac{\kappa}{2}\right)^2\beta^2}. \tag{159}$$

We get the same bound when $\frac{\kappa}{2}$ is odd. Indeed, in this case $n_e=\frac{1}{2}\left(\frac{\kappa}{2}-1\right)=\frac{\kappa}{4}-\frac{1}{2}$ (now half the numbers between 1 and $\frac{\kappa}{2}-1$, inclusive, are even), and $n_o=\left(\frac{\kappa}{2}-1\right)-n_e=\frac{\kappa}{4}-\frac{1}{2}$. Then (157) also becomes

$$\frac{1}{\kappa}\sqrt{\left(\frac{1}{m}+2\left(\frac{\kappa}{4}-\frac{1}{2}\right)\beta\right)^2+\beta^2\left(1+2\left(\frac{\kappa}{4}-\frac{1}{2}\right)\right)^2} \tag{160}$$

$$=\frac{1}{\kappa}\sqrt{\left(\frac{1}{m}+\left(\frac{\kappa}{2}-1\right)\beta\right)^2+\left(\frac{\kappa}{2}\right)^2\beta^2}. \tag{161}$$

This concludes the proof. ■

Remark: If were to mimic the proof of Theorem 4 in the case when m is even (so $-1\in A$ and the c_x^d are real), then we would arrive at the same bound as in Theorem 14. Indeed, in this case from Lemma 15 we have

$$\left(\gamma^{-(i-1)(j-1)}w_j\right)^*=\gamma^{-(i-1)((\kappa-j+2)-1)}w_{\kappa-j+2}, \tag{162}$$

for $j=2,...,\kappa$, and hence if κ is odd we have

$$c_{x^{i-1}}=\frac{1}{\kappa}\sum_{j=1}^{\kappa}\gamma^{-(i-1)(j-1)}w_j \tag{163}$$

$$=\frac{1}{\kappa}\left[w_1+\sum_{j=2}^{\frac{\kappa+1}{2}}\left(\gamma^{-(i-1)(j-1)}w_j+\gamma^{-(i-1)((\kappa-j+2)-1)}w_{\kappa-j+2}\right)\right] \tag{164}$$

$$=\frac{1}{\kappa}\left[-\frac{1}{m}+\sum_{j=2}^{\frac{\kappa+1}{2}}2\beta\cos(\tilde{\theta}_j)\right]. \tag{165}$$

If κ is even, we note that our above condition (162) implies that $\left(\gamma^{-(i-1)\frac{\kappa}{2}} w_{\frac{\kappa}{2}+1}\right)^* = \gamma^{-(i-1)\frac{\kappa}{2}} w_{\frac{\kappa}{2}+1}$, so we must have that $\gamma^{-(i-1)\frac{\kappa}{2}} w_{\frac{\kappa}{2}+1}$ is real, and hence equal to $\pm\beta$. Thus we get

$$c_{x^{i-1}} = \frac{1}{\kappa}\left[w_1 + \gamma^{-(i-1)\frac{\kappa}{2}} w_{\frac{\kappa}{2}+1} + \sum_{j=2}^{\frac{\kappa}{2}} \left(\gamma^{-(i-1)(j-1)} w_j + \gamma^{-(i-1)((\kappa-j+2)-1)} w_{\kappa-j+2}\right)\right] \tag{166}$$

$$= \frac{1}{\kappa}\left[-\frac{1}{m} \pm \beta + \sum_{j=2}^{\frac{\kappa}{2}} 2\beta\cos(\tilde{\theta}_j)\right]. \tag{167}$$

In either case, maximizing over $\{\theta_j\}$ gives us an upper bound of

$$\mu \leq \frac{1}{\kappa}\left(\frac{1}{m} + (\kappa-1)\beta\right), \tag{168}$$

which matches with our bound from Theorem 14.

References

[1] W. U. Bajwa, R. Calderbank, S. Jafarpour, "Why Gabor frames? Two fundamental measures of coherence and their role in model selection," *J. Commun. Netw.*, 12: 289-307, 2010.

[2] J. Benedetto and M. Fickus, "Finite Normalized Tight Frames," Advances in Computational Mathematics 18 (2-4), 357-385, 2003.

[3] E. R. Berlekamp, "The weight enumerators for certain sub codes of the second order binary Reed-Muller codes," *Inform. Control* 17, 485-500, 1970.

[4] E. J. Candes, "The restricted isometry property and its implications in compressed sensing," *C. R. Acad. Sci. Paris S'er. I Math.* 346, 589-592, 2008.

[5] E. J. Candes, J. Romberg and T. Tao, "Stable signal recovery from incomplete and inaccurate measurements," *Comm. Pure Appl. Math.* 59, 1208-1223, 2006.

[6] E. J. Candes and T. Tao, "Decoding by linear programming," *IEEE Trans. Inform. Th.* 51, 4203-4215, 2005.

[7] P. G. Casazza, "The Art of Frame Theory," Taiwanese Journal of Mathematics Vol. 4, No. 2, pp. 129-201, June 2000.

[8] P. G. Casazza, M. Fickus, D. G. Mixon, Y. Wang, Z. Zhou, "Constructing tight fusion frames," Applied and Computational Harmonic Analysis 30 (2), 175-187, 2011.

[9] P. G. Casazza and J. Kova?eviȁc, "Equal-norm tight frames with erasures," *Advances in Computational Mathematics*, Springer, 2003.

[10] P.G. Casazza and G. Kutyniok, "Finite Frames: Theory and Applications," Chapter 5 (written by S. Waldron). Springer, 2012.

[11] P. G. Casazza and G. Kutyniok, "Frames of Subspaces," Wavelets, Frames and Operator Theory, Contemp. Math., College Park, MD, 2003, vol. 345, Amer. Math. Soc., Providence, RI pp. 87-113, 2004.

[12] P. G. Casazza, G. Kutyniok, and S. Li, "Fusion frames and distributed processing," Applied and Computational Harmonic Analysis, Vol. 25, Iss. 1, pp. 114-132, July 2008.

[13] T. Chien, S. Waldron, “A classification of the harmonic frames up to unitary equivalence,” Appl. Comput. Harmon. Anal. 30, 307-318, 2011.

[14] P. Delsarte, J. M. Goethals and J. J. Seidel, “Spherical Codes and Designs,” *Geometriae Dedicata*, Vol. 6, No. 3, 363-388, 1977.

[15] C. Ding, “Complex codebooks from combinatorial designs,” IEEE Trans. Inf. Theory, vol. 52, no. 9, pp. 4229-4235, Sep. 2006.

[16] C. Ding and T. Feng, “A Generic Construction of Complex Codebooks Meeting the Welch Bound,” IEEE Transactions on Information Theory, Vol. 53 , Issue 11, 2007.

[17] D. L. Donoho and M. Elad, “Optimally sparse representations in general (non-orthogonal) dictionaries via ℓ_1 minimization,” *Proc. Nat. Acad. Sci.* 100, 2197-2202, 2002.

[18] D. L. Donoho and X. Huo, “Uncertainty principles and ideal atomic decompositions,” *IEEE Trans. Inform. Theory* 47, 2845-2862, 2001.

[19] T. C. Eldar and G. D. Forney, Jr., “Optimal tight frames and quantum measurement,” *IEEE Trans. Inform. Theory*, 48, 599-610, 2002.

[20] J. L. Fan, “Array codes as Low-Density Parity Check codes,” *Proc. Int'l. Symp. on Turbo Codes*, Brest, France, 543-546, Sept. 2000.

[21] M. Fickus, D. G. Mixon, J. C. Tremain, “Steiner equiangular tight frames,” Linear algebra and its applications 436 (5), 1014-1027, 2012.

[22] N. Hay, S. Waldron, “On computing all harmonic frames of n vectors in $\mathbb{C}^d$,” Appl. Comput. Harmon. Anal. 21, 168-181, 2006.

[23] R. W. Heath, Jr., H. Bolcskei and A.J Paulraj, “Space-time signaling and frame theory,” *IEEE Proceedings of ICASSP*, 4, 2445-2448, 2001.

[24] R. W. Heath, Jr. and A. J. Paulraj, “Linear dispersion codes for MIMO systems based on frame theory,” *IEEE Trans. on Sig. Proc.* Vol. 50, Issue 10, 2429-2441, 2002.

[25] D. G. Mixon, W. U. Bajwa, and R. Calderbank, “Frame Coherence and Sparse Signal Processing,” *Proceedings of ISIT*, 2011.

[26] A. Prasad, Representations of $GL_2(\mathbb{F}_q)$ and $SL_2(\mathbb{F}_q)$, and some remarks about $GL_n(\mathbb{F}_q)$. Lecture Notes, Advanced Instructional School on Representation Theory and Related Topics heldat the Bhaskaracharya Pratishthana and the University of Pune, July 2007.

[27] M. Reeder. Characters of $SL_2(q)$. https://www2.bc.edu/ reederma/SL(2,q).pdf?, December 2008.

[28] J. M. Renes, R. Blume-Kohout, A. J. Scott, C. M. Caves, “Symmetric informationally complete quantum measurements,” J. Math. Phys. 45, 2171-2180, 2004.

[29] A. J. Scott, “Tight informationally complete quantum measurements,” *J. Phys. A: Math. Gen.* **39** 13507, 2006.

[30] J. P. Serre and L. L. Scott, “Linear Representations of Finite Groups,” Graduate Texts in Mathematics, Springer, New York, 1977.

[31] D. Slepian, “Group Codes for the Gaussian Channel,” *Bell Sys. Tech. J.*, vol. 47, pp. 575-602, Apr. 1968.

[32] T. Strohmer and R. W. Heath Jr., “Grassmannian frames with appications to coding and communication,” *Appl. Comput. Harmon. Anal.* 14, 257-275, 2003.

[33] S. Tanaka. Construction and classification of irreducible representations of special linear group of the second order over a finite field. *Osaka J. Math*, 4:65-84, 1967.

[34] A. Terras, “Fourier Analysis on Finite Groups and Applications. Cambridge: Cambridge University Press, 1999.

[35] M. Thill and B. Hassibi, “Frames, Group Codes, and Subgroups of $(\mathbb{Z}/p\mathbb{Z})^{\times}$,” *Proc. of Allerton 2012.*

[36] M. Thill and B. Hassibi, “Frames from Groups: Generalized Bounds and Dihedral Groups,” ICASSP 2013.

[37] M. Thill and B. Hassibi, “Group Frames with Few Distinct Inner Products and Low Coherence,” submitted to IEEE Transactions on Signal Processing.

[38] M. Thill and B. Hassibi, “On frames from abelian group codes,” Proceedings of ISIT, 2013.

[39] M. Thill, V. Muthakumar and B. Hassibi, “Frames from Generalized Group Fourier Transforms and $SL_2(\mathbb{F}_q)$,” ICASSP 2014.

[40] J. Tropp and A. Gilbert, “Signal recovery from partial information via orthogonal matching pursuit,” *IEEE Trans. Inform. Theory*, vol. 53, no. 12, pp. 4655-4666, 2007.

[41] R. Vale, S. Waldron, “The symmetry group of a finite frame,” Linear Algebra Appl. 433, 248- 262, 2010.

[42] R. Vale and S. Waldron, “Tight frames and their symmetries,” *Constr. Approx.* 21, 83-112, 2005.

[43] R. Vale, S. Waldron, “Tight frames generated by finite nonabelian groups,” Numer. Algorithms 48, 11-27, 2008.

[44] S. Waldron, “An Introduction to Finite Tight Frames,” Springer, NewYork, 2011.

[45] W. D. Wallis, “Combinatorial Designs,” Marcel Dekker, New York, 1988.

[46] L. Welch, “Lower bounds on the maximum cross correlation of signals,” IEEE Trans. Inf. Theory, vol. 20, no. 3, pp. 397-399, May 1974.

[47] P. Xia, S. Zhou, G. B. Giannakis, “Achieving the Welch bound with difference sets,” *IEEE Trans. Inform. Theory* 51, 1900-1907, 2005.

[48] N. Y. Yu and G. Gong, “A new binary sequence family with low correlation and large size,” *IEEE Trans. Inform. Theory* 52, 1624-1636, 2006.